Beyond Unbundling: A Capacity Development Framework for Equipping Polytechnic Lecturers and Technologists to Deliver Practice-Based Computing Skills in Nigeria

Folusho Olayinka Owoeye [1], Oluwakemi Sade Ayodele [2], Oluwabukola Inubiwon Oluwaseyi [3]

[1,2,3] Department of Computer Science, Kogi State Polytechnic, Lokoja

Abstract

The National Board for Technical Education unbundled the Higher National Diploma in Computer Science in January 2024, replacing the single award with four specialised programmes in artificial intelligence, networking and cloud computing, software and web development, and cybersecurity and data protection. The reform aims to produce graduates whose skills meet current industry needs, but curriculum documents alone cannot deliver it. Lecturers and technologists must be trained to teach the content to the standard industry expects. This conceptual paper uses documentary policy analysis of regulatory circulars, agency communications, national policy instruments and research on vocational teacher development to ask whether Nigerian polytechnics hold that capability and to interrogate the prevailing response of certifying staff as instructors under partnerships with Cisco and Huawei. The three capacity routes compared are higher degrees, vendor certification and industry-led train-the-trainer provision. Six capacity deficits are identified namely, live practice on real equipment, pedagogical conversion, production experience, role differentiation between cadres, competency assessment, and unrewarded industrial skill. The paper proposes the Practice Capacity Framework, a six-pillar structure that treats vendor certification as an entry tier rather than a terminal qualification and adds supervised live sessions on real equipment, differentiated technologist pathways, and a proposed Trainers' Industrial Work Experience Scheme modelled on SIWES. It is offered as a proposition for empirical testing rather than a validated model.

Keywords: technical and vocational education, polytechnic education, lecturer capacity development, industry collaboration, train-the-trainer, Nigeria

1. INTRODUCTION

Nigerian technical education entered a period of structural revision when the National Board for Technical Education (NBTE) circulated a letter dated 8 January 2024 announcing the unbundling of the Higher National Diploma (HND) in Computer Science. Four replacement programmes were established: HND Artificial Intelligence, HND Networking and Cloud Computing, HND Software and Web Development, and HND Cybersecurity and Data Protection. Admissions into the former generalist programme ceased from the 2024/2025 session, with institutions given until 2025 to graduate students already enrolled (Ayeni & Shaibu, 2024). The stated rationale was to position graduates more strategically for national development.

The reasoning is defensible. A single computing award covering databases, networks, programming, hardware maintenance and emerging technologies within a two-year diploma cycle produces graduates with broad familiarity and thin capability, whereas specialisation permits deeper treatment of a defined competence set. The National Information Technology Development Agency welcomed the restructuring (Digital Times Nigeria, 2024), and the change aligns with the National Digital Economy Policy and Strategy (Federal Republic of Nigeria, 2020), the National Digital Literacy Framework (National Information Technology Development Agency, 2023), and the commitment that technical education should produce employable skill rather than certificates alone (Federal Republic of Nigeria, 2013).

Specialisation on paper does not guarantee specialised capability in a graduate. What converts a curriculum into competence is teaching staff working in functioning laboratories, using current toolchains, assessing student work against standards industry recognises. Two analytical propositions follow, advanced as propositions rather than documented national facts, since no comprehensive audit of Nigerian polytechnic computing staff qualifications or laboratory provision appears to be publicly available. The first is that a substantial proportion of computing lecturers earned their qualifications under the generalist regime the reform has replaced. The second is that laboratory provision in many institutions was specified for an earlier generation of practical work, consistent with findings on workshop facility utilisation in Nigerian technical institutions (Ya'u et al., 2025; Wordu & Chiorlu, 2017). If either holds, a lecturer who has not deployed a production workload to a cloud platform is poorly placed to supervise a student doing so, and a technologist without current virtualisation skills will struggle to keep a laboratory functional beyond the accreditation visit. Establishing their extent is among the empirical questions in Section 6.

The NBTE has recognised this dependency and acted on it. In September 2024 the Board launched a programme with Cisco Academy, delivered through the University of Jos Cisco Academy, to equip more than 500 computer science lecturers from 113 institutions to implement the new programmes; participation was announced as a prerequisite for resource inspection and accreditation, with a further round signalled for artificial intelligence (National Board for Technical Education (NBTE), 2024). A parallel arrangement with Huawei, reported as covering student training across 21 polytechnics with dual certification, was signed in Abuja in August 2023 (Daily Trust, 2023; Vanguard, 2023); NBTE making both Cisco and Huawei as part of the requirements for resource inspection and course accreditation (NBTE, 2024). Those completing such programmes may become certified instructors, authorised to create courses on vendor platforms, enrol students and teach.

Vendor academies supply curricula, simulators, assessment banks and international recognition, and tying participation to accreditation gave staff development an institutional weight it has rarely carried. The partnerships are best understood as a launchpad. The question is what should be built on it, because the reform has been managed as a curriculum and certification exercise when it is an institutional workforce problem. Certification establishes that a participant passed a vendor assessment. It does not establish that the participant can build and sustain a working laboratory, demonstrate a procedure on real equipment while students watch, supervise a student through failure and revision, or assess a functioning artefact. Previous studies has repeatedly identified the absence of such capabilities as a driver of graduate unemployability (Otache, 2022).

A second route is already in heavy use, whereby staff upgrade through higher degrees. The investment is rational and the qualifications valuable, but they answer a different question from the one the unbundled programmes pose. A research degree is awarded principally for demonstrated capacity to conduct and report original enquiry; it does not ordinarily assess whether the holder can configure a current cloud environment, operate a deployment pipeline or lead an incident response, and the divergence is likely to be wider in computing because industrial tools turn over faster than a research degree takes to complete. Between the two routes sits a missing third: industry led provision teaching the skills employers are hiring for, delivered live on real equipment.

The programme was convened virtually and its practical content, in common with vendor academy models generally, is carried substantially by simulation software. Simulation does this work well, being safe and a sound starting point, but it cannot give the entire experience gained with real tools. The argument here is therefore additive rather than corrective: simulation should remain, and live sessions on real equipment should follow it.

Three research questions were used as a roadmap for the analysis:

1. What capacities do polytechnic lecturers and technologists require in order to deliver the four unbundled HND computing programmes at a standard that produces demonstrable practical competence in graduates?
2. To what extent does the vendor instructor training model exemplified by the NBTE partnerships with Cisco and Huawei address those capacities?
3. What institutional framework can combine academic upgrading, vendor certification and industry collaboration into sustained, practice-based teaching capability within Nigerian polytechnics?

The paper makes two contributions. Academically, it treats technologists as partners in skill delivery rather than support staff, a distinction the polytechnic scheme of service formalises but research has largely overlooked. The study also brings evidence on the acquisition of practical skill to bear on a Nigerian policy question. Practically, it offers a sequenced framework identifying which capacity investments must precede others.

2. RELATED WORKS

Unbundling divides a broad qualification into narrower awards, each with a defined occupational orientation, trading breadth for depth so that the remaining hours are spent on fewer competences taught to a higher standard. It is common in vocational systems that align qualifications to occupational standards rather than academic disciplines.

Specialisation raises the technical demand on the lecturer, since the generalist treatment a broad syllabus permits is no longer acceptable. A department teaching HND Cybersecurity and Data Protection must field staff who can operate intrusion detection systems and reason about data protection compliance. Unbundling therefore raises the staffing threshold at the same moment that it narrows the curriculum, and where the threshold is unmet the reform yields specialised titles attached to unchanged teaching. European manufacturing education offers one model of what closing that threshold involves. The teaching factory approach organises instruction around two-way exchange between institution and firm, so that live industrial problems enter the teaching environment and staff remain participants in the practice they teach (Chryssolouris et al., 2016).

The institutional response to that threshold has, in computing, long run through the vendor academy. Vendor-based curricula have shaped computing education for decades. The Cisco Networking Academy distributes a centrally developed curriculum with standards-based online assessment delivered by locally and internationally trained instructors, and reports Nigerian enrolment exceeding 540,000 students since operations began in 2000 (NBTE, 2024). Huawei operates a comparable structure through its ICT Academy programme.

The advantages are clear: students graduate holding both a national award and an internationally recognised credential. The critique is equally established. Where a vendor supplies the materials and the examination, quality becomes dependent on the vendor rather than institutional academic judgement. Scope is a second limitation, since vendor curricula are product-oriented by design and do not teach design reasoning, requirements negotiation, debugging under uncertainty or client communication. The UNESCO-UNEVOC International Centre for Technical and Vocational Education and Training (UNESCO-UNEVOC, 2022) found that many technical and vocational teaching staff internationally lacked the digital skills and delivery experience for technology-mediated instruction, reporting that only 18 per cent of providers in low-income countries sustained remote learning during the pandemic. Possession of technical content is not the same as capability to deliver it.

If certification does not by itself settle the question of capability, the prior question is how practical competence is acquired at all. Competence of the kind the four programmes name is acquired by doing, under conditions resembling those in which it will later be exercised, and two strands of evidence bear on how far provision must go to secure it.

The first concerns structured practice environments. Simulation tools support active learning and give immediate feedback, making individual practice possible at cohort sizes enterprise equipment could never accommodate. Cisco Packet Tracer is well established on these grounds, and its adoption in resource-constrained settings is sound (Allison, 2022). Any realistic Nigerian provision will rest on such tools.

The second concerns what those environments must lead to. Marquardson and Gomillion (2019) had students complete a configuration exercise in a simulated environment, then repeat it on physical routers and switches. Self-efficacy rose significantly after the first, but difficulty concentrated in physical operations such as cabling, power connection, port selection, console access and configuration reset. They concluded that practice environments should augment work with physical equipment rather than substitute for it. The study is small, seventeen participants at one institution, so its findings are indicative. Its value lies in identifying which competences require live conditions, and they are largely the ones a technologist exercise daily.

Previous studies documents a persistent separation between polytechnic teaching and industrial practice. Otache (2022), drawing on focus group discussions with polytechnic lecturers, NBTE officials and industry executives, found graduate unemployability attributable in part to a wide collaboration gap between institutions and industry, and identified the need to involve industry experts in curriculum development and in teaching specified curriculum components. Notably for the present argument, participants identified the desirability of exposing lecturers, and not only students, to industrial work situations. Work placement learning has similarly been associated with student employability (Otache & Edopkolor, 2022).

The Nigerian polytechnic system maintains a formal distinction between the academic and technologist cadres, the latter charged with laboratory and workshop operation, equipment maintenance and supervision of practical sessions. Research on Nigerian technical institutions has associated under-utilisation of workshop equipment with inadequate availability and training of technical personnel, and has linked poor practical skill acquisition to facilities that are present but not operationally maintained (Ya'u et al., 2025; Wordu & Chiorlu, 2017). Laboratory capability is therefore a staffing question before it is a procurement question. The prevailing route to staff development is academic upgrading. Conditions of service tie promotion to qualifications and publications, so staff pursue higher degrees as the reliable path to advancement, and the workforce gains research credentials while the currency of its industrial practice goes unmeasured. The capacity route the system funds and the capacity the unbundled programmes require are therefore not the same route, and neither substitutes for the other.

Taken together, these literatures identify the elements of the problem without addressing the problem itself. The literature was located through structured searching of Google Scholar, ERIC, African Journals Online and the UNESCO-UNEVOC repository, combining terms for the policy object (curriculum unbundling, specialisation, HND, polytechnic, TVET), the population (lecturer, trainer, technologist), the intervention (capacity development, vendor certification, industrial attachment, train-the-trainer) and the setting (Nigeria, Africa). Searches were unrestricted by date for theoretical sources and restricted to 2015 onwards for empirical and policy material, with backward and forward citation searching until no further relevant items appeared.

That process located three well-populated bodies of work and one gap. Previous studies from Nigeria address curriculum relevance, industry collaboration and workshop facility utilisation; previous international studies address vendor certification and technical teacher development in general terms; computing education research addresses how practical skill is acquired and where it transfers. No retrieved study examined the institutional problem created when a regulator unbundles a programme and simultaneously routes the resulting staff development requirement through a small number of technology vendors. Two further absences were noted: the technologist cadre appears largely as a resourcing variable rather than a population with its own development pathway, and no study compared academic upgrading, vendor certification and industry engagement as alternative capacity routes. This paper addresses those gaps. The claim is that no such treatment was located by the search described yet.

3. THEORETICAL FRAMEWORK

The paper draws on three complementary bodies of theory. Shulman (1986) argued that effective teaching depends on pedagogical content knowledge, distinct from subject knowledge, concerning how content is represented, sequenced and made learnable, and Mishra and Koehler (2006) extended this to technology-mediated teaching, treating technology, pedagogy and content as interacting domains. A vendor certification certifies technological content knowledge alone, leaving untouched the pedagogical and integrative components a lecturer needs to convert a syllabus into teaching that produces competent students.

Desimone (2009) identified core features of professional development that changes practice: content focus, active learning, coherence, sufficient duration and collective participation. Later synthesis added modelling, expert coaching and structured reflection (Darling-Hammond et al., 2017). Collectively these literatures provide an evaluative standard for the NBTE arrangements and a design specification for what should supplement them. Guskey (2002) adds that teachers change their beliefs after observing improved student outcomes, not before, a dynamic reinforced by mastery experience in professional self-efficacy (Bandura, 1997).

Lave and Wenger (1991) and Wenger (1998) situate learning within communities of practice, holding that competence develops through participation rather than transmission of decontextualised knowledge, and Billett (2001) shows that a work setting's learning value depends on how far it affords participation in consequential tasks. Lecturers and technologists are therefore likely to acquire production-grade capability by participating in real technical work, and communities of practice across polytechnics offer a low-cost means of sustaining it between training rounds.

These perspectives combine to generate the framework in Section 5.6. The content and pedagogical content knowledge distinction (Shulman, 1986; Mishra & Koehler, 2006) separates what a certification supplies from what it cannot, so certified technical currency becomes an entry tier (Pillar 1) and pedagogical conversion a separate stage (Pillar 3). The core features of effective professional development, extended to modelling and coaching (Desimone, 2009; Darling-Hammond et al., 2017), specify the form conversion takes, hence demonstration under observation and departmental peer review in Pillars 2 and 3. Situated learning and workplace affordance (Lave & Wenger, 1991; Billett, 2001) justify supervised live practice (Pillar 2) and two-way industry collaboration (Pillar 5). Constructive alignment (Biggs, 1996) and assessment's durable influence on behaviour (Boud & Falchikov, 2006) generate artefact-based assessment (Pillar 6). Guskey (2002) and Bandura (1997) explain the sequencing, since staff sustain new practice only after seeing it succeed, and Fullan (2016) supports the governance layer. Pillar 4 is the one component the borrowed theory does not generate; it follows from the occupational analysis in Section 5.1, the scheme of service, and evidence on workshop facility utilisation (Ya'u et al., 2025; Wordu & Chiorlu, 2017).

4. METHODOLOGY

4.1 Study design

This is a conceptual paper employing documentary policy analysis. It generates no primary empirical data and makes no claims contingent on statistical inference. The design suits an implementation that is ongoing and an analytical task of framework construction rather than hypothesis testing. The framework in Section 5 should be read as a proposition for empirical testing rather than a validated model.

Because conceptual work of this kind moves between what documents establish, what the authors infer and what the authors propose, these three registers are signalled consistently throughout. Statements of documented fact are attributed to a named source. Inferences drawn by the authors are marked by hedged formulations such as suggests, indicates or is likely to. Proposals are introduced as such, using the language of should or is proposed.

4.2 Documentary corpus

Documents were assembled between January 2024, when the unbundling circular was issued, and the time of writing. Table 1 lists the corpus by category, indicating what each category was used to establish.

Table 1: Documentary corpus and evidential function

Category	Documents	Used to establish
Regulatory and agency	NBTE unbundling circular of 8 January 2024 as reported in the national press; NBTE communication on the Cisco initiative, September 2024.	Programme titles, dates, phase-out, participant and institution numbers, accreditation linkage.
Partnership and comparative	Huawei corporate account of the Kenya train-the-trainer agreement; press reporting of the NBTE–Huawei memorandum and of the Kenyan second phase.	Design features of vendor train-the-trainer arrangements in Nigeria and a comparable African system.
National policy	National Digital Economy Policy and Strategy 2020–2030; National Digital Literacy Framework; National Policy on Education.	Policy environment against which coherence is judged.
Scholarly	Research on vocational teacher development, polytechnic-industry collaboration, vendor curricula, workshop facility utilisation and the acquisition of practical skill; UNESCO-UNEVOC trends analysis.	Theoretical grounding and comparative evidence.

Source: compiled by the authors.

Three inclusion criteria were applied: traceability to an identifiable institutional, corporate or scholarly source; direct bearing on at least one research question; and, for matters of public record, corroboration by a second independent source or an official communication. Press reports were used only for dates, programme titles, participant numbers and reported terms, and are identified as such at each point of use. Where official documentation was sought but could not be retrieved, this is stated rather than concealed.

4.3 Analytical procedure

Analysis proceeded in four stages, generating four analytical categories that structure Section 5. The first reconstructed policy intent from the regulatory documents, establishing what the four programmes are expected to produce. The second derived from the occupational content of each programme, the staff capacities required for credible delivery, distinguishing lecturer from technologist requirements and produced the category of practice requirements reported in Table 2. The third compared those requirements against what the prevailing capacity routes supply, using the core features of effective professional development (Desimone, 2009) as the evaluative lens, and produced the categories of conditions requiring live delivery and of capacity routes, reported in Tables 3 and 4. The fourth grouped the residual shortfalls into six deficits and mapped each to a corresponding response, producing the six pillars. The mapping is one deficit to one pillar, with the governance layer addressing conditions on which all six depend, and Figure 1 represents the structure.

4.4 Criteria for framework development

The framework was constructed against four criteria. The first is affordability within realistic polytechnic budgets. The second is enforceability through instruments the NBTE already controls, principally accreditation and resource inspection. The third is the explicit treatment of technologists as well as lecturers. The fourth is sequencing, so that institutions with limited resources know what to build first.

4.5 Limitations of the approach

Documentary analysis captures what institutions state, not what they do. The paper cannot report how many participants completed the Cisco training, what proportion subsequently taught the new programmes, or whether laboratory provision changed as a result. Section 6 proposes these as the priority research agenda.

A second limitation concerns source availability. Full programme documentation for the Nigerian vendor partnerships is not publicly retrievable, so the live contact time participants received, and whether institutions supplemented the programme locally, are not on record. Official documentation of the NBTE–Huawei memorandum could not be obtained, and the account rests on corroborated press reporting, which is flagged wherever used. Conclusions are framed to hold wherever such contact time was limited, without asserting figures that cannot be evidenced.

A third limitation attaches to the supporting evidence. Marquardson and Gomillion (2019) worked with seventeen students at one North American institution, so their findings are indicative rather than an effect size transportable to Nigeria, and the Kenyan comparison illustrates a design option rather than demonstrating an outcome, since no independent evaluation of its effects was located.

5. ANALYSIS AND DISCUSSION

5.1 What the unbundled programmes demand of lecturers and technologists

Table 2 maps the four programmes to the competences a graduate would be expected to demonstrate and the laboratory conditions without which they cannot be taught.

Table 2: Practice requirements of the unbundled HND computing programmes

Programme	Core practice competences	Laboratory and toolchain conditions	Technologist responsibility
Artificial Intelligence	Data preparation, model training and evaluation, deployment of a working model, ethical and data governance reasoning.	Compute for model training, Python data science stack, versioned datasets, notebook environment.	Compute scheduling, environment reproducibility, dataset storage and integrity,
Networking and Cloud Computing	Network design and configuration, routing and switching, cloud resource provisioning, monitoring and cost control.	Physical or emulated network equipment, virtualisation host, sponsored or free-tier cloud accounts.	Virtualisation host maintenance, topology reset between cohorts, account and quota administration.

Programme	Core practice competences	Laboratory and toolchain conditions	Technologist responsibility
Software and Web Development	Requirements analysis, version-controlled development, testing, deployment, collaborative working.	Development machines, version control server or hosted equivalent, continuous integration, staging deployment target.	Toolchain provisioning, repository administration, build environment support.
Cybersecurity and Data Protection	Vulnerability assessment, incident detection and response, forensic acquisition, compliance analysis under Nigerian and international law.	Isolated laboratory segment, deliberately vulnerable targets, monitoring and forensic tooling.	Network isolation, safe target maintenance, evidence handling.

Source: derived by the authors from the programme titles established in the NBTE circular (Ayeni & Shaibu, 2024).

The study identified that every programme requires an actively maintained laboratory and the maintenance burden falls on the technologist cadre. And the competences in the second column are performances rather than propositions: they are demonstrated by producing something that works, so they must be taught by someone who has done so and assessed by evidence of production rather than written examination.

5.2 The vendor instructor model

Assessed against Desimone's (2009) core features, the arrangements perform unevenly. On content focus they perform well, since the curricula are technically current and industry-aligned. On collective participation they perform reasonably, since staff attended as institutional representatives drawn from 113 institutions, creating conditions for departmental rather than individual change (NBTE, 2024). On coherence they perform adequately, since the training was aligned to the new curricula and tied to accreditation.

On active learning and duration, the position is weaker. Vendor instructor training certifies technical knowledge through vendor examinations. It is not directed at teaching practice and does not typically include observation of the participant teaching or feedback on instructional design, and its duration is bounded by the certification track rather than by the time practice takes to change. Guskey's (2002) point applies: a participant who gains a certificate but sees no improvement in student outcomes has no experiential basis for altering long-standing habits.

Coverage is a further issue. The September 2024 initiative addressed three of the four programmes, with artificial intelligence announced as a later round (NBTE, 2024), so the programme with the least established teaching tradition was the last to receive support, reversing the order capability logic would suggest. This is not a criticism of the partnerships but an argument for widening them, since no single vendor's portfolio maps onto all four specialisations equally well.

The participation of technologists deserves accurate statement, because their exclusion is easy to assume. They were not excluded; institutions nominated their own participants and a number sent technologists alongside lecturers. The difficulty lies elsewhere. Nomination was discretionary rather than structured, so coverage of the technical cadre depended on how each institution read the invitation, and a technologist sitting the same certification track as a lecturer acquires the same configuration knowledge, which is not the capability to build a laboratory environment, document its configuration, restore it between cohorts and keep it operating for a semester. Inclusion occurred; role differentiation did not.

5.3 Onsite training for laboratory competences

Participants hold recent, industry-aligned knowledge of architectures, protocols, configuration and tooling, and the online format achieved a reach that physical convening across 113 institutions would not have allowed. What remains is the competence only live conditions produce. The empirically identified points of difficulty are physical and operational: cabling, power connection, port selection, console access, and restoring a device to a known state between exercises (Marquardson & Gomillion, 2019). These consume a technologist's working day and must be diagnosed in front of a class. The equivalents elsewhere are a live cloud account that generates a bill, a deployment that fails only on the target, data that arrives with its defects intact, and an incident that does not follow a script. Table 3 separates, for each programme, what current provision secures from what requires live conditions.

Table 3: Competences secured by current provision and competences requiring live conditions

Programme	Secured by current provision	Requiring real equipment, platforms or workloads
Networking and Cloud Computing	Topology design, addressing schemes, routing and switching syntax, protocol behaviour	Cabling and termination, port and transceiver faults, console access, device reset, live cloud billing, quota exhaustion, throughput under load
Cybersecurity and Data Protection	Attack taxonomies, tool syntax, scripted scenarios, compliance concepts	Live traffic capture, unscripted incident behaviour, forensic acquisition from real media, evidence handling, isolation of a compromised segment
Software and Web Development	Language syntax, framework structure, algorithm design, version control commands	Builds that fail only on the target, merge conflicts between people, dependency breakage, staging and production deployment, code review
Artificial Intelligence	Model architectures, training procedure, evaluation metrics, notebook workflow	Messy and imbalanced real data, labelling disputes, compute scheduling and cost, deployment and monitoring

Source: developed by the authors, drawing on Marquardson and Gomillion (2019).

The right-hand column lists ordinary professional conditions rather than advanced topics. The two columns are sequential rather than opposed: the left is the necessary foundation, the right converts it into competence an employer can use, and provision stopping at the left leaves the conversion undone.

5.4 Staff capacity routes

Nigerian polytechnic staff currently develop through two routes, and the framework below adds a third. They are not competitors, since each produces something the others do not. Table 4 sets out what each delivers.

Table 4: Comparison of the three routes to lecturer and technologist capacity

Route	What it develops	What it does not develop	Institutional position
Higher degrees (MSc, PhD)	Research capability, theoretical depth, supervision of student projects, disciplinary credibility.	Current industrial practice, tool currency, operational and physical competence.	Rewarded by promotion criteria and the dominant route in practice.
Vendor certification	Technically current, industry-aligned knowledge of architectures, protocols and configuration.	Teaching capability, live equipment competence, role-specific technologist skill, practice beyond the vendor's product range.	Recently mandated for accreditation by NBTE, with broad reach at low unit cost.
Industry-led train-the-trainer	In-demand employer skills, live equipment and workload practice, current toolchains and workplace conduct.	Research capability and disciplinary breadth beyond the specialisation.	Largely absent in Nigeria; the gap this paper identifies

Source: developed by the authors.

A polytechnic whose staff hold doctorates and vendor certificates may still have nobody who has recently worked the way hiring employers work. A vendor is a technology supplier and its academy teaches its own product range to a defined standard, which is appropriate to what a vendor is. The firms hiring polytechnic graduates in Nigeria are diverse, including software houses, fintechs, banks, operators, data centres, security consultancies and startups, few of them built on a single vendor stack. Knowledge of what those employers use, and how they work, sits with their practitioners rather than with curriculum documents or vendor syllabi, and industry-delivered train-the-trainer brings it into the institution faster than either other route.

A regional precedent exists for the delivery mode. Under an agreement between Huawei and Kenya's Ministry of Education State Department for Vocational and Technical Training, launched in July 2021, a train-the-trainer programme began with 25 lecturers from ten national polytechnics, delivered by Huawei-certified trainers in a continuous ten-day block and concluding in certification, with student training to follow. The sequencing was explicit at the launch, the Assistant Director for Vocational and Technical Education describing the building of trainer capacity first as the condition for implementing the programme (Huawei Kenya, 2021). The scheme has since been institutionalised through the Kenya School of TVET, and its second phase is reported to have taken 65 lecturers through a fifteen-day course covering artificial intelligence, data communication, cloud technologies and cybersecurity, with most returning to operationalise ICT academies in their own institutions (Kenya Broadcasting Corporation, 2025; Capital FM, 2025). The specialisations correspond closely to Nigeria's four, and two design features are instructive: duration measured in continuous days rather than hours dispersed across a term, and a designated national centre concentrating equipment where it can be used repeatedly. The comparison illustrates a design option rather than demonstrating an outcome, since no independent evaluation of its effect was located.

5.5 Six residual capacity deficits

The analysis identifies six deficits that vendor instructor certification, as currently delivered, does not address. The first is the live practice deficit, where participants gained current technical knowledge without sustained contact with the equipment and platforms their students must handle. A lecturer cannot demonstrate what the lecturer has not performed, and demonstration is the central instructional act in practical teaching. A technologist cannot maintain what the technologist has not built, and a laboratory nobody can restore after the first serious fault stops supporting teaching for the rest of the semester. The remedy is additive: retain the practice environments that work and add supervised live sessions after them (Marquardson & Gomillion, 2019).

The second is the pedagogical deficit. Converting technical knowledge into a semester of instruction requires a different competence: sequencing tasks by difficulty, designing projects that fail productively, diagnosing the misconception behind a student's error and giving feedback on work in progress. Mishra and Koehler (2006) treat this integrative capacity as irreducible to technical or pedagogical knowledge alone, and Schön (1987) locates much of it in coaching reflection within the act of practising. Nothing in a vendor certification track develops it.

The third is the production experience deficit. Vendor curricula teach configuration within controlled scenarios, whereas professional practice involves ambiguous requirements, legacy constraints, incomplete documentation and consequences for failure. A lecturer who has only worked inside vendor scenarios is poorly placed to supervise a project that meets conditions the scenario excluded. Otache's (2022) participants identified exposure of lecturers to industrial work as a need distinct from student placement, though its value depends on the placement being structured so the participant moves between workplace activity and analysis of it rather than merely observing (Guile & Griffiths, 2001; Kolb, 1984).

The fourth is the role differentiation deficit. All four programmes depend on environments requiring continuous maintenance rather than periodic procurement; a virtualisation host that fails in week six ends practical teaching for the semester. No publicly available technologist curriculum was located that addressed environment build documentation, restoration between cohorts, fault logging or the isolation procedures a security laboratory requires. On the available evidence, the cadre with the clearest operational mandate received the least role-specific preparation.

The fifth is the assessment deficit. If competence is a performance, assessment must examine performance: a deployed application, a configured and documented network, an incident response report, a trained model with an evaluation record. This is constructive alignment, under which tasks elicit the performances the outcomes describe rather than a proxy (Biggs, 1996), and it matters because assessment shapes what students do long after the course ends (Boud & Falchikov, 2006). Vendor examinations assess the vendor's content, not the student's ability to produce work under the conditions the programme title implies.

The sixth is the incentive and qualification-currency deficit. Promotion criteria include publication and higher degrees, not the maintenance of a working laboratory, the supervision of a live client project or a current professional certification. Staff invest rationally in the route that advances them, so the system accumulates research credentials while industrial skill goes unmeasured. The remedy is not to devalue higher degrees, which serve a real purpose, but to give industrial currency comparable standing so that staff need not choose between advancement and industry skill.

5.6 The Practice Capacity Framework

The framework organises the response into six pillars over a governance layer that conditions all of them. The pillars are sequenced, each depending on those before it, so institutions with constrained resources should build them in order.

Figure 1 represents the structure.

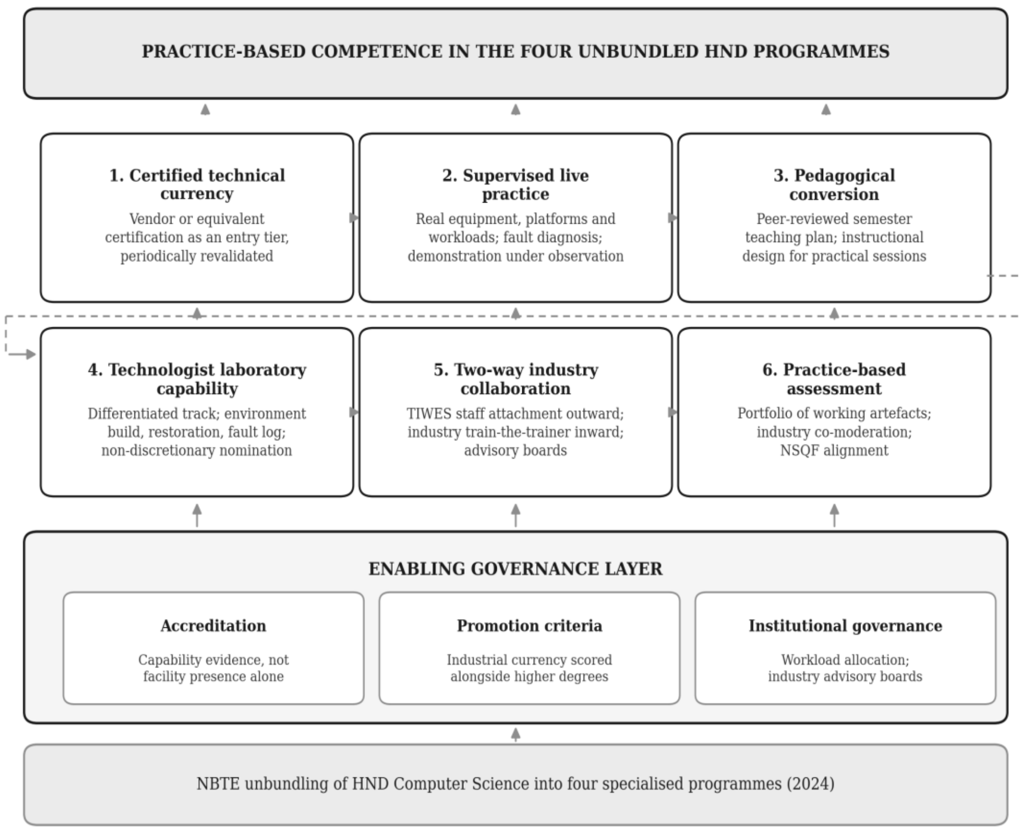


Figure 1: The Practice Capacity Framework (*Solid arrows indicate the proposed build sequence; the broken arrow marks continuation from the upper to the lower row of pillars). Source: developed by the authors.*

Pillar 1: Certified technical currency**.** This is the existing vendor arrangement, repositioned. The requirement that participation precede resource inspection should be retained but recast as an entry threshold rather than evidence of teaching readiness, and certification should carry a currency period requiring revalidation, since a 2024 cloud certification will not describe 2028 practice. Vendor selection should be diversified so that no single stack defines a national curriculum.

Pillar 2: Supervised live practice on real equipment. Every participant completing a certification track should then complete a supervised block of live sessions on real equipment before being counted ready to deliver the programme, adding to the present arrangement rather than displacing it. Three features matter. Sequence comes first: structured practice environments should precede live work, the order the evidence supports (Marquardson & Gomillion, 2019), so that participants arrive holding the configuration knowledge and contact time goes to what only live conditions teach. Content follows the right-hand column of Table 3, covering cabling, console access, device reset and fault injection in networking; a live cloud account with a real budget; a staging deployment, merge conflict and code review in software development; live traffic capture and an unscripted incident in cybersecurity; and an uncurated dataset in artificial intelligence. Third is demonstration-based teaching, where the participant demonstrates the procedure aloud to peers under observation and receives feedback on the demonstration itself, addressing the pedagogical deficit within the same block at no additional cost and supplying the modelling and coaching the evidence identifies as decisive (Darling-Hammond et al., 2017; Desimone, 2009). Delivery need not be uniform: zonal centres hosted by institutions or industry partners that already hold equipment can serve clusters on rotation, and a transportable rack moved between them reaches more staff than any fixed facility.

Pillar 3: Pedagogical conversion and teaching design. Beyond the demonstration in Pillar 2, every participant should produce a semester teaching plan specifying the practical sessions, the laboratory conditions each requires and the artefacts students will produce, peer reviewed by departmental colleagues rather than submitted for a further certificate. Peer review satisfies Desimone's (2009) collective participation condition and begins a departmental community of practice at negligible marginal cost.

Pillar 4: Technologist-specific laboratory capability. This treats the technologist cadre as a delivery agent. Nomination should cease to be discretionary, so that each institution mounting one of the programmes enrols technologists on a differentiated track covering virtualisation and container administration, network laboratory build and restoration, cloud account and quota administration, and cybersecurity laboratory isolation.

Two elements complete the pillar. The first is a documented laboratory operations regime comprising environment build documentation, a reset procedure between cohorts, a maintenance schedule and a fault log, held by the technologist and inspected at accreditation. The second is a substitution strategy for what cannot be afforded outright: emulation running genuine device firmware, container-based rather than licensed development environments, educational cloud credits, decommissioned enterprise equipment donated by operators and banks, and shared regional facilities for compute-intensive workloads. Accreditation should assess whether a laboratory has been operating, evidenced by the fault log and session records, not merely whether equipment is present.

Pillar 5: Two-way industry collaboration**.** This pillar carries the traffic in both directions, and both directions are necessary. Nigeria already operates a mature instrument for moving learners into workplaces, the Students Industrial Work Experience Scheme, and the proposal here applies that logic to the people who teach. It is termed the Trainers' Industrial Work Experience Scheme, abbreviated TIWES. No such scheme currently exists; TIWES is a policy model proposed by the authors, named to signal a sibling of SIWES rather than a new bureaucracy, and using the term trainers because the eligible population includes both cadres. Table 5 sets out the proposed design parameters, offered as a starting specification for consultation rather than settled policy.

Table 5: Proposed design parameters for the Trainers' Industrial Work Experience Scheme

Parameter	Proposed provision	Rationale and feasibility considerations
Eligibility and cycle	Lecturers and technologists in the four specialisations; a continuous block of not less than four weeks every three years.	Shorter attachments are unlikely to survive induction; a three-year cycle matches toolchain turnover and limits simultaneous absence.
Administration	Industrial Training Fund as administrator, NBTE specifying competence expectations, institutional SIWES units handling logistics.	Reuses machinery that already serves students, avoiding a new agency and reducing set-up cost.
Funding	ITF employer levy, supplemented by institutional staff development votes and in-kind partner contributions such as host supervision and equipment access.	Requires no new revenue instrument, but the levy's governing provisions would need review to confirm staff attachment is admissible.
Employer participation	Voluntary hosting incentivised by levy reimbursement or offset, formalised in a memorandum covering supervision, confidentiality and intellectual property.	Employer willingness is untested and is the principal feasibility risk, confidentiality being a live concern in security and financial placements.
Assessment	A defined work output agreed at the outset, countersigned by the host supervisor, with a reflective account submitted to the department.	Distinguishes attachment from observation and produces inspectable evidence.
Monitoring	Institutional register of completions, sampled NBTE verification at accreditation, periodic reporting of participation by specialisation.	Uses an existing inspection point rather than a separate audit regime.
Legal and institutional basis	Amended conditions of service recognising attachment as scoreable; an NBTE circular establishing the requirement; an ITF operational guideline.	The instruments required are administrative rather than legislative, lowering the barrier to adoption.

Source: proposed by the authors.

Where placement is impractical, sustained contribution to an open-source project under maintainer review offers a verifiable alternative for the software and data specialisations. TIWES is argued to return three dividends. The immediate return is current skill, since staff acquire the tools and working practices their students will meet, consistent with the situated learning position that capability develops through participation rather than description (Lave & Wenger, 1991). The second is research relevance, since staff pursuing higher degrees would carry back problems the industry has, so that theses address questions employers recognise; the attachment makes the doctorate more useful and the doctorate gives the attachment analytical depth, reconciling the two routes of Section 4.4. The third is professional formation, since ethics, client confidentiality, documentation discipline and escalation conduct are more readily transmitted by people recently held to them. These are reasoned expectations rather than demonstrated effects, and evaluating them forms part of the research agenda in Section 6.

The vendor partnerships should continue and, following the Kenyan example, deepen towards intensive in-person delivery. Alongside them, practising engineers, analysts, architects and data scientists from Nigerian firms should be engaged as train-the-trainer instructors delivering live sessions on the skills their firms are hiring for. This widens the technology base beyond any single vendor's range, reaches staff who cannot be released for placement, and transmits the practitioner's judgement about which approach is presently preferred and why, which Otache's (2022) participants identified as a remedy for the collaboration gap. Delivery should be concentrated in blocks of continuous days at a designated zonal centre with equipment available (Huawei Kenya, 2021; Kenya Broadcasting Corporation, 2025), sustained by a departmental industry advisory board for each specialisation that reviews curriculum currency and nominates the practitioners who deliver each cycle.

Pillar 6: Practice-based assessment. Each programme should carry a mandatory portfolio component in which the student submits working artefacts with documentation and a reflective account of the decisions taken. Criteria should be published, moderated across institutions and mapped to the National Skills Qualifications Framework so the evidence is portable, with external moderation including at least one industry practitioner. This pillar depends on Pillar 4, since portfolio work needs a laboratory, somebody keeps operational, and on Pillars 2 and 3, since staff must be able to perform, demonstrate and moderate such work before it is required of them.

The six pillars will not hold without three enabling changes. Promotion criteria should score verified industrial placement, current certification and documented laboratory development alongside higher degrees and publication. Teaching load allocation should account for the preparation laboratory-based instruction requires. And accreditation should extend beyond facility presence to capability evidence: staff certifications, live training completion records, laboratory operations documentation and moderated student portfolios. Accreditation is the Board's most effective lever and the instrument through which the framework becomes enforceable rather than aspirational, though reform adopted in form but not in practice fails unless the capacity of implementers is built deliberately (Fullan, 2016). Table 6 summarises the differentiated pathways for the two staff cadres.

Table 6: Differentiated capacity pathways by staff cadre

Capacity domain	Lecturer pathway	Technologist pathway	Evidence of attainment
Technical currency	Vendor or equivalent certification in the specialisation, revalidated periodically	Differentiated certification in virtualisation, systems and laboratory administration	Valid certificate with currency date
Live practice competence	Supervised block on real equipment; fault diagnosis; live platform exposure	Supervised environment build, cabling, restoration and fault injection	Trainer sign-off against a task list
Pedagogy and delivery	Demonstration teaching under observation; peer-reviewed teaching plan	Practical session facilitation and student safety briefing	Observed demonstration; approved semester teaching plan
Production experience	Structured industrial placement with defined output	Structured placement in a data centre or operations environment	Placement report countersigned by host supervisor
Laboratory capability	Specification of laboratory requirements for the teaching plan	Environment build, reset, maintenance and fault management	Laboratory operations file inspected at accreditation
Assessment	Design and moderation of portfolio assessment	Verification that submitted artefacts function in the target environment	Moderated portfolio sample with industry co-assessor

Source: compiled by the authors.

5.7 Implications and constraints

Theoretically, vendor certification maps onto Shulman's (1986) content knowledge and onto the technological component of the Mishra and Koehler (2006) framework, but the pedagogical and integrative components remain the institution's responsibility and cannot be procured externally. Reform strategies treating vendor partnership as a complete solution conflate one component with the whole.

For policy, treating academic upgrading, vendor certification and industry train-the-trainer as three routes with defined yields allows an institution to audit which its staff have travelled and to invest in the one that is missing, and most are likely to find the third largely untravelled. The routes reinforce rather than rival one another, since industrial attachment supplies research questions employers recognise, so that the higher degrees staff already pursue produce work industry can use. In practice the question is sequencing under scarcity. An institution that certifies its lecturers but cannot maintain a laboratory has purchased credentials rather than capability, and a polytechnic with a functioning laboratory and industrially experienced staff is likely to produce better graduates than the reverse. Where budgets force a choice, Pillars 2 and 4 deserve priority over additional certification volume.

Live delivery is its most expensive element and hardest to scale, which is why the online model was adopted; the zonal centre and rotating equipment proposals attempt to contain that cost. Industrial placement and train-the-trainer at national scale presume employer willingness that has not been tested and would require incentives, possibly through the Industrial Training Fund levy. Electricity supply and bandwidth costs affect laboratory operation in ways no training programme can resolve. Attrition may rise as capability improves, which argues for institutionalising capability in documented systems rather than individuals. And the framework assumes a regulator willing to make accreditation more demanding when many institutions already struggle with existing standards.

6. RECOMMENDATIONS AND CONCLUSION

Five recommendations follow, each addressed to an instrument the regulator or institutions already control. First, the vendor programme should be extended with a compulsory block of live sessions on physical equipment and platforms at zonal centres serving clusters of institutions, with completion of that block, rather than the certificate alone, becoming the accreditation prerequisite. Second, that block should require each participant to demonstrate a procedure aloud under observation, so that instructional capability is assessed alongside technical capability. Third, nomination of technologists should cease to be discretionary, with every institution mounting one of the programmes enrolling a named technologist on a differentiated track and the resulting laboratory operations file inspected at accreditation. Fourth, the NBTE should extend the partnership model into a national industry-led train-the-trainer scheme drawing on the wider Nigerian technology ecosystem alongside the current vendor partners, governed by departmental industry advisory boards. Fifth, the proposed Trainers' Industrial Work Experience Scheme should be established through the Industrial Training Fund, and promotion criteria revised so that industrial currency carries weight alongside higher degrees and publications. Because the framework is a reasoned proposition rather than a tested model, five questions merit priority in future research: how much live contact time participants received and whether institutions supplemented the programme locally; how many participants subsequently taught the new programmes, and with what change in practice; what proportion of institutions nominated technologists, and what those technologists could do afterwards; the operational status of computing laboratories across a representative sample of institutions; and what the first graduating cohorts can demonstrably do on equipment they have not seen before. A replication of the Marquardson and Gomillion (2019) transfer design with Nigerian polytechnic staff and students would answer the first at modest cost.

The unbundling of HND Computer Science addressed a genuine defect, and four specialised programmes offer a better structure for producing employable graduates than one generalist award covering an expanding field. Its success rests on a condition the curriculum revision could not itself create, namely the capability of the lecturers and technologists who must deliver it. The NBTE's partnerships with Cisco and Huawei are a creditable first response and should continue, since they establish that external technical organisations can be engaged in polytechnic staff development at national scale. The analysis indicates that they are not sufficient alone, and neither is academic upgrading, which builds research capability rather than industrial currency. Six capacity deficits are identified across the two prevailing routes, and the Practice Capacity Framework proposes a response to each, positioning vendor certification as an entry tier, adding supervised live practice and demonstration teaching, and giving technologists a pathway matched to the work they perform. Until the empirical questions above are addressed, the judgements advanced here remain provisional.

REFERENCES

Allison, J. (2022). Simulation-based learning via Cisco Packet Tracer to enhance the teaching of computer networks. In *Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education* (Vol. 1, pp. 68–74). Association for Computing Machinery. https://doi.org/10.1145/3502718.3524739

Ayeni, V., & Shaibu, N. (2024, January 13). NBTE unbundles HND Computer Science. *Punch*. https://punchng.com/nbte-unbundles-hnd-computer-science/

Bandura, A. (1997). *Self-efficacy: The exercise of control*. W. H. Freeman.

Biggs, J. (1996). Enhancing teaching through constructive alignment. *Higher Education*, *32*(3), 347–364. https://doi.org/10.1007/BF00138871

Billett, S. (2001). *Learning In The Workplace: Strategies for effective practice (1st ed.)*. Routledge. https://doi.org/10.4324/9781003116318

Boud, D., & Falchikov, N. (2006). Aligning assessment with long-term learning. *Assessment & Evaluation in Higher Education*, *31*(4), 399–413. https://doi.org/10.1080/02602930600679050

Capital FM. (2025, December 5). *Kenya moves to deepen digital skills partnership with Huawei as 65 TVET lecturers complete advanced ICT training*. https://capitalfm.africa/kenya-moves-to-deepen-digital-skills-partnership-with-huawei-as-65-tvet-lecturers-complete-advanced-ict-training/

Chryssolouris, G., Mavrikios, D., & Rentzos, L. (2016). The teaching factory: A manufacturing education paradigm. *Procedia CIRP*, *57*, 44–48. https://doi.org/10.1016/j.procir.2016.11.009

Daily Trust. (2023, August 18). *Huawei to train students in 21 polytechnics on ICT skills*. https://dailytrust.com/huawei-to-train-students-in-21-polytechnics-on-ict-skills/

Darling-Hammond, L., Hyler, M. E., & Gardner, M. (2017). *Effective teacher professional development*. Learning Policy Institute. https://learningpolicyinstitute.org/product/effective-teacher-professional-development-report

Desimone, L. M. (2009). Improving impact studies of teachers' professional development: Toward better conceptualizations and measures. *Educational Researcher*, *38*(3), 181–199. https://doi.org/10.3102/0013189X08331140

Digital Times Nigeria. (2024, January 16). *NITDA commends NBTE's recent unbundling of HND Computer Science programme*. https://digitaltimesng.com/nitda-commends-nbtes-recent-unbundling-of-hnd-computer-science-programme/

Federal Republic of Nigeria. (2013). *National policy on education* (6th ed.). NERDC Press.

Federal Republic of Nigeria. (2020). *National digital economy policy and strategy (2020–2030)*. Federal Ministry of Communications and Digital Economy. https://nitda.gov.ng/wp-content/uploads/2020/06/National-Digital-Economy-Policy-and-Strategy.pdf

Fullan, M. (2016). *The new meaning of educational change* (5th ed.). Teachers College Press.

Guile, D., & Griffiths, T. (2001). Learning through work experience. *Journal of Education and Work*, *14*(1), 113–131.

https://doi.org/10.1080/13639080020028738

Guskey, T. R. (2002). Professional development and teacher change. *Teachers and Teaching*, *8*(3), 381–391. https://doi.org/10.1080/135406002100000512

Huawei Kenya. (2021). *Vocational schools boosted as 25 TVET lecturers begin advanced technology training to increase the occupational prospects of TVET graduates* https://www.huawei.com/ke/news/2020/vocational%20schools%20boosted%20as%2025%20tvet%20lecturers%20begin%20advanced%20technology%20training

Kenya Broadcasting Corporation. (2025, December 4). *Kenya School of TVET, Huawei complete 2nd phase of national ICT lecturer capacity building program*. https://www.kbc.co.ke/kenya-school-of-tvet-huawei-complete-2nd-phase-of-national-ict-lecturer-capacity-building-program/

Kolb, D. A. (1984). *Experiential learning: Experience as the source of learning and development*. Prentice Hall.

Lave, J., & Wenger, E. (1991). *Situated learning: Legitimate peripheral participation*. Cambridge University Press.

Marquardson, J., & Gomillion, D. L. (2019). Simulation for network education: Transferring networking skills between simulated to physical environments. *Information Systems Education Journal*, *17*(1), 28–39. https://isedj.org/2019-17/n1/ISEDJv17n1p28.html

Mishra, P., & Koehler, M. J. (2006). Technological pedagogical content knowledge: A framework for teacher knowledge. *Teachers College Record*, *108*(6), 1017–1054. https://doi.org/10.1111/j.1467-9620.2006.00684.x

National Board for Technical Education. (2024, September 2). *NBTE partners with Cisco to train over 500 computer science lecturers on new HND programmes*. https://web.nbte.gov.ng/node/74

National Information Technology Development Agency. (2023). *National digital literacy framework*. https://nitda.gov.ng/wp-content/uploads/2023/07/Digital-Literacy-Framework.pdf

Otache, I. (2022). Enhancing graduates' employability through polytechnic–industry collaboration. *Industry and Higher Education*, *36*(5), 604–614. https://doi.org/10.1177/09504222211063140

Otache, I., & Edopkolor, J. E. (2022). Work placement learning and student employability: Do student satisfaction, commitment and achievement matter? *Industry and Higher Education*. Advance online publication. https://doi.org/10.1177/09504222221091989

Schön, D. A. (1987). *Educating the reflective practitioner*. Jossey-Bass.

Shulman, L. S. (1986). Those who understand: Knowledge growth in teaching. *Educational Researcher*, *15*(2), 4–14. https://doi.org/10.3102/0013189X015002004

UNESCO-UNEVOC International Centre for Technical and Vocational Education and Training. (2022). *Trends mapping study: Digital skills development in TVET teacher training*. https://unevoc.unesco.org/pub/trends_mapping_study_digital_skills_development_in_tvet_teacher_training.pdf

Vanguard. (2023, August 18). *Tech firm, Huawei hosts Teachers Summit, signs MoU with*

NBTE, Uniport. https://www.vanguardngr.com/2023/08/tech-firm-huawei-hosts-teachers-summit-signs-mou-with-nbte-uniport/

Wenger, E. (1998). *Communities of practice: Learning, meaning, and identity*. Cambridge University Press.

Wordu, C. C. R., & Chiorlu, D. O. (2017). Utilization of workshop equipment and tools for the improvement of teaching and learning of technical vocational education and training (TVET) in technical colleges in Nigeria. *Journal of Scientific and Engineering Research*, *4*(6), 127–131.

Ya'u, R., Nafiu, I., Rabiu, B. A., & Nura, S. A. (2025). An appraisal of workshop facilities and equipment utilization for teaching and learning of metal work in technical education of Kano State, Nigeria. *Kashere Journal of Education*, *9*(2), 68–75.

Vibe Coding and Artificial Intelligence: A Narrative Review of Software and Web Development Training in Nigerian Polytechnics

Folusho Olayinka Owoeye [1], Oloruntoba Leke Joseph [2], Oluwakemi Sade Ayodele [3]
[1,3]Department of Computer Science, [2]Department of Computer Engineering, Kogi State Polytechnic, Lokoja
owoeyefolusho@kogistatepolytechnic.edu.ng

Abstract

The National Board for Technical Education unbundled the Higher National Diploma in Computer Science into specialised streams, one of which prepares students for software and web development. The reform coincided with the arrival of generative artificial intelligence in ordinary programming practice, popularised as vibe coding, in which working applications are produced from natural language prompting rather than direct code authorship. Students on the programme have begun to ask their lecturers whether two years of study will still hold value at graduation. This study addresses that question through a two-strand design: a document analysis of the approved curriculum, treated as primary data, supported by a targeted review of empirical and policy literature. Ninety-two prescribed credit units were coded against a three-category rubric distinguishing codified implementation content from foundation content and from content concerned with specification, verification, security and professional accountability. Just under one fifth of prescribed credit load falls in the codified implementation category, while over half falls in the third. Reviewed evidence indicates that generative assistance redistributes engineering effort rather than removing it, that practitioners frequently judge generated code fast but flawed, and that experienced developers retain control rather than delegating it. Available evidence suggests the programme remains relevant in an AI-assisted development environment, particularly where training emphasises code comprehension, software design, testing, security, system integration and verification. Recommendations are offered for students, polytechnics and the regulator, and are framed as propositions requiring empirical validation in the Nigerian setting.

Keywords: Vibe coding, AI-assisted programming, HND Software and Web Development, code comprehension, curriculum analysis, Nigerian polytechnics

1. INTRODUCTION

Nigeria's information and communication sector has become one of the more visible contributors to national output, accounting for 11.18 per cent of real gross domestic product in the second quarter of 2025 (National Bureau of Statistics, 2025). Expansion on this scale creates demand for people who can build and maintain digital products, and a substantial part of that demand is met by the polytechnic system rather than by universities alone, since technical education is charged with producing technologists for direct entry into industry. Whether the system supplies the skills employers want has been questioned for some time. Otache (2022) reported that Nigerian polytechnic graduates reach the labour market with limited exposure to genuine workplace conditions, and argued for closer institutional collaboration with industry as the corrective.

The National Board for Technical Education addressed part of this concern by restructuring computing provision at the Higher National Diploma level. The single HND Computer Science curriculum was unbundled into specialised programmes, among them Cyber Security and Data Protection, Networking and Cloud Computing, Software and Web Development, and Artificial Intelligence (National Board for Technical Education [NBTE], 2024). The Software and Web Development curriculum was approved in September 2023 and prescribes a two-year programme of four semesters and a minimum of ninety credit units, in which practical work carries fifty per cent of the assessment weight against fifty per cent for theory (NBTE, 2023). From September 2024 more than five hundred computer science lecturers drawn from one hundred and thirteen institutions were trained through Cisco Academy to deliver the unbundled programmes, and completion of that training was made a condition of accreditation resource inspection (NBTE, 2024). The reform is neither provisional nor lightly resourced, and it commits institutions to a defined body of content for the accreditation cycle ahead.

Its timing invites attention. The curriculum was approved as large language models capable of producing working source code passed from research demonstration into ordinary developer practice. By early 2025 the practice had acquired a popular name, attributed to a widely circulated post by Karpathy (2025) describing a way of working in which the developer states an intention in ordinary language, accepts what the model returns, and ceases to attend to the code itself. Adoption is no longer marginal. Eighty-four per cent of respondents to the Stack Overflow (2025) developer survey reported using or intending to use artificial intelligence tools in their work, against seventy-six per cent a year earlier, even as the proportion trusting the accuracy of the output fell from forty per cent to twenty-nine per cent.

Students on the programme have drawn the obvious inference and have begun to voice it in programming classes. Their question is whether an employer will pay a graduate to write PHP endpoints or manipulate the Document Object Model when a language model returns comparable output in seconds. It is not a naive question, and lecturers presently answer it from intuition rather than from evidence. The concern has a precise curricular anchor. Front End Development I and II and Back End Development I and II together carry twelve credit units and twenty-four hours of scheduled practical work, and their stated objectives centre on HTML structure, styling, JavaScript syntax, the Document Object Model, PHP data types and control structures, string manipulation and basic error handling (NBTE, 2023). These are among the task categories on which code generation performs most reliably. The programme also carries Artificial Intelligence as a shared three-unit course in the first semester, drawn from the parallel Artificial Intelligence curriculum, which places the subject inside the programme from the outset.

Existing scholarship does not settle the matter. Research on generative artificial intelligence in computing education has concentrated on introductory university programming, on assessment integrity and on instructor practice (B. A. Becker et al., 2023; Prather et al., 2023; Denny et al., 2024). A small but growing empirical literature now addresses vibe coding directly (Fawzy et al., 2026; Gama et al., 2026; Huang et al., 2025; Sarkar & Drosos, 2025), though it examines professional practitioners, university undergraduates and practitioner discourse rather than technical and vocational diploma programmes. Evidence on developer productivity is divided, with a controlled experiment reporting substantial task acceleration (Peng et al., 2023) and a later trial with experienced practitioners reporting the opposite (J. Becker et al., 2025). Labour market evidence of contraction among early-career workers in exposed occupations has begun to appear, though it is drawn from United States payroll records (Brynjolfsson et al., 2025). None of this work examines a Nigerian technical education programme, and no published study analyses the NBTE Software and Web Development curriculum as a document with specified competencies and assessment weightings. That absence defines the gap addressed here.

Three questions guide the study:

1. Which competencies specified in the HND Software and Web Development curriculum are most exposed to substitution by generative artificial intelligence, and which are complemented by it?
2. What does available empirical evidence indicate about entry-level prospects in software and web occupations under conditions of widespread artificial intelligence adoption?
3. Which artificial intelligence competencies should graduates acquire alongside the approved curriculum in order to work more productively and strengthen their labour market position?

The study matters on three counts. Students entering the programme make a two-year commitment and deserve an answer grounded in evidence rather than reassurance or alarm. Programme managers and the regulator face an accreditation cycle in which approved content will be inspected against industry practice, and a documented account of where exposure and complementarity fall informs that process. For scholarship, the study offers the first systematic analysis of an unbundled Nigerian technical computing curriculum against the capabilities of code-generating systems, and supplies a coding method transferable to the parallel streams.

2. REVIEW METHODOLOGY AND RELATED WORKS

2.1 Review Approach and Study Design

2.1.1 Research design

This study employs a two-strand qualitative design. The primary strand is a document analysis of the approved curriculum for the Higher National Diploma in Software and Web Development (NBTE, 2023), treated as primary data rather than as background. The secondary strand is a targeted review of empirical, educational and policy literature, conducted to establish the capability profile of generative code-generating systems against which curriculum content is assessed.

A fully systematic protocol assumes a body of studies homogeneous enough for pooled appraisal, and no such body yet exists for this question, since the relevant evidence spans randomised experiments, security assessments, practitioner surveys, payroll analyses, grey literature syntheses and curriculum documents. Locating primary evidence in a public regulatory document, rather than in an aggregate of heterogeneous studies, produces a claim any reader may reproduce by obtaining the same document and applying the stated rubric. The literature strand is accordingly targeted and purposive rather than exhaustive, and no claim of comprehensive coverage is made.

2.1.2 Curriculum document analysis

The analysis uses the Higher National Diploma (HND) Software and Web Development:

Curriculum and Course Specifications, approved by the National Board for Technical Education in September 2023 and comprising 269 pages (NBTE, 2023). The document is publicly available through the Board's curriculum portal. The unit of analysis is the individual prescribed course. The curriculum specifies thirty-two courses across four semesters, totalling ninety-two credit units against a prescribed minimum of ninety.

For each course the following were extracted verbatim: course code and title, credit units, lecture and practical contact hours, prerequisites, stated goal, and stated general objectives. Courses shared with parallel programmes, and courses whose specifications are issued separately, were coded from their curriculum table entries and stated titles. Each course was assigned to one of three categories according to the decision rules in Table 1. The rules operationalise the theoretical distinction developed in Section 2.4, under which substitution pressure follows from the codification of a task rather than from its routineness.

Table 1

Coding rubric for classification of prescribed courses

Category	Assignment rule	Applied when
A. Codified implementation	Assigned when all three conditions hold	(i) stated objectives centre on producing code or artefacts for well-specified problems; (ii) canonical solutions are abundantly represented in public code corpora; (iii) correctness is verifiable by inspection or straightforward execution
B. Foundation and enabling	Assigned when either condition holds	(i) the course supplies underpinning knowledge whose primary instructional function is comprehension of system behaviour rather than production of a deliverable; (ii) stated objectives combine codified production with contextual or hardware constraint
C. Specification, verification and accountability	Assigned when any condition holds	(i) objectives require eliciting or negotiating context not contained in the artefact; (ii) objectives require judgement among competing constraints; (iii) the course assigns professional or ethical accountability; (iv) the course concerns verification, security, communication, research or enterprise

Note. Where a course's stated general objectives spanned more than one category, it was assigned to the category matching the majority of those objectives. Where objectives divided evenly, the course was assigned to Category B as the conservative option, since Category B makes no claim in either direction.

Coding was performed by the first author against the rubric in Table 1, working from the extracted objective statements rather than from course titles. Fourteen of the thirty-two courses were unambiguous on the first pass. Nine required application of the majority rule, and three were assigned to Category B under the even-split provision. Independent double coding was not conducted, and inter-rater reliability was therefore not computed. This is a material limitation, disclosed in Section 2.1.4 and revisited in Section 4.3, where independent expert rating is proposed as the immediate next study.

Category totals were obtained by summing the prescribed credit units of member courses. Percentages express each category total as a proportion of the ninety-two prescribed units, rounded to one decimal place. The figures describe curriculum load only, and Section 3.1 states explicitly what they do and do not license.

2.1.3 Literature identification and selection

Literature was identified through targeted searching of the ACM Digital Library, IEEE Xplore, arXiv, Google Scholar and African Journals Online, together with the official publications of the National Board for Technical Education, the National Bureau of Statistics and the World Economic Forum. Search strings paired technology terms, rendered as "vibe coding" OR "AI code generation" OR "large language model" OR "GitHub Copilot" OR "generative AI", with domain terms, rendered as "programming education" OR "software engineering" OR "developer productivity" OR employability OR curriculum. Nigerian material was sought separately by pairing polytechnic OR "technical education" OR NBTE with computing OR "computer science" OR employability.

Sources were included where they reported empirical findings, systematic or grey literature syntheses, or official policy and statistical positions; appeared in English; and addressed at least one research question. The date range 2003 to 2026 admits the theoretical framework at its lower bound. Vendor marketing material, opinion commentary unsupported by data, and secondary reporting of primary studies were excluded, the last because several claims circulating in secondary reporting could not be traced to a retrievable primary source and were dropped rather than cited. Practitioner survey evidence was admitted where the instrument and sampling were disclosed, with self-selection noted at the point of use. Twenty-two sources were retained, distributed as shown in Table 2.

Table 2

Sources retained, by type and contribution

Source type	n	Contribution to the study
Peer-reviewed conference and journal papers.	9	Capability, quality and security profile of generated code; computing education evidence; theoretical framework.
Preprints and working papers.	4	Productivity experiments; labour market analysis; agentic system architectures.
Official curriculum and regulatory documents.	2	Primary data and programme context.
National statistical publications.	2	Nigerian macroeconomic and labour market context.

Source type	n	Contribution to the study
International organisation reports.	1	Global employer skill demand.
Practitioner survey.	1	Adoption, trust and verification burden.
Grey literature synthesis.	1	Practitioner accounts of vibe coding.
Originating source of the term.	1	Definitional provenance.
Nigerian higher education scholarship.	1	Graduate employability context.

Note. Counts reflect sources retained after screening. The literature strand is purposive rather than exhaustive; see Section 2.1.4.

2.1.4 Limitations of the method

Four limitations follow from the design. First, the literature strand was screened by a single reviewer without independent double screening and without a formal quality appraisal instrument, so selection bias cannot be excluded. Second, the curriculum coding was performed by one coder, so no inter-rater reliability statistic is available and the classification should be treated as a transparent and reproducible proposal rather than a validated instrument. Third, credit units measure prescribed instructional load and carry no information about labour market value. Fourth, the capabilities under assessment change quickly, which time-stamps the analysis to the period of writing.

2.2 Conceptual Review

Discussion in this area frequently treats all machine assistance as equivalent. The modes differ materially in the degree of human comprehension retained, and therefore in their risk profile. Table 3 distinguishes them.

Table 3

Modes of AI-assisted software development, by comprehension retained

Mode	Description	Comprehension retained
Code completion	Model suggests the continuation of a line or block being typed.	High
Prompting for code	Developer requests a specific fragment and integrates it deliberately.	High
AI pair programming	Model proposes, developer reviews and accepts or rejects each change.	High
Natural-language-to-code generation	Whole components generated from a written specification, then reviewed.	Moderate

Mode	Description	Comprehension retained
Agentic software development	Model plans and executes multi-step changes across files under supervision.	Moderate to low
Vibe coding	Developer accepts output without reading it, iterating by trial and outcome.	Low by definition
Autonomous software engineering	System specifies, implements and validates with minimal human involvement.	Not yet established in practice

Note. Ordering reflects comprehension retained rather than technical sophistication. The table was adapted by the authors from descriptions in Karpathy (2025), Sarkar and Drosos (2025), Fawzy et al. (2026) and Huang et al. (2025).

Vibe coding should be understood as an emerging and contested term rather than a settled academic construct. It originates in a social media post (Karpathy, 2025) and entered research papers only afterwards. Sarkar and Drosos (2025) provided an early empirical treatment through analysis of extended recorded sessions, framing the practice as programming through conversation and noting the questions it raises about expertise and programmer agency. Fawzy et al. (2026), synthesising 101 practitioner sources and 518 accounts, define it as reliance on generation through intuition and trial and error without necessarily understanding the underlying code. This study adopts that definition, and treats the defining feature as the deliberate suspension of code comprehension rather than the use of artificial intelligence as such.

The distinction matters for what follows. A developer who can read, trace and reason about generated output operates a tool and remains accountable for the result. A developer who cannot is dependent on it. The value of a programming course under these conditions lies less in the speed of syntax production, a contest already conceded, than in the capacity to understand what was produced.

2.3 Empirical Review

Evidence on productivity points in two directions, and the reconciliation is instructive. Peng et al. (2023) recruited developers to implement an HTTP server in JavaScript and found the group with access to an assistant completed the task 55.8 per cent faster than the control group, with larger benefits accruing to less experienced participants. J. Becker et al. (2025) reached an apparently contrary result: working with sixteen experienced open-source developers across 246 tasks in mature repositories already familiar to them, completion took nineteen per cent longer when tools were permitted, although participants believed afterwards that they had been twenty per cent faster.

These findings are compatible once task character is considered. The first examined a self-contained problem with a clear specification and abundant precedent in public code. The second examined incremental work inside large familiar contexts where establishing whether a suggestion fits costs more than writing the change. Fawzy et al. (2026) reach a compatible conclusion from practitioner accounts, describing a speed and quality trade-off in which generation is experienced as rapid yet the resulting code is widely judged fast but flawed. Their synthesis reports that quality assurance is frequently omitted, with users skipping testing or delegating verification back to the generating tool, and identifies a resulting class of developers able to build a product but unable to debug it when it fails.

Pearce et al. (2022) constructed eighty-nine scenarios and examined 1,689 generated programs, finding approximately two fifths contained weaknesses corresponding to recognised vulnerability classes. Practitioner experience aligns: in the Stack Overflow (2025) survey, sixty-six per cent of respondents reported that generated answers were almost right but not quite, and forty-five per cent reported losing significant working time correcting them.

Huang et al. (2025) combined field observation of thirteen developers with a survey of ninety-nine, found that professionals value agents for productivity but retain agency over design and implementation, employing deliberate strategies to constrain agent behaviour that draw on their own expertise. Their participants reported confidence in working with agents precisely because they could compensate for agent limitations. Expertise, on this evidence, is what makes the tools usable rather than what the tools displace.

Computing education research has responded chiefly with concern about assessment integrity and about novices bypassing the productive difficulty through which comprehension forms (B. A. Becker et al., 2023; Prather et al., 2023; Denny et al., 2024). Gama et al. (2026) provide the most directly relevant empirical study, observing thirty-one undergraduates in nine teams at a Brazilian public university during a one-day vibe coding hackathon. Participants achieved rapid prototyping, cross-disciplinary collaboration and functional demonstrations, and developed prompting skill. The study also observed premature convergence during ideation, uneven code quality requiring rework, and limited engagement with core software engineering practice, concluding that human judgement remained essential for critical refinement and that such settings work best when scaffolded by explicit instruction in critical evaluation of output.

Two boundaries qualify this literature for present purposes. It examines university programmes rather than technical and vocational diploma provision, and with the partial exception of Gama et al. (2026), it is drawn from high-income settings. No study located here addresses a Nigerian institution. Brynjolfsson et al. (2025), analysing United States payroll records, reported a sixteen per cent relative employment decline among workers aged twenty-two to twenty-five in the most exposed occupations, with employment stable among more experienced workers in the same occupations. Set against this, the World Economic Forum (2025), surveying more than one thousand employers representing some fourteen million workers across fifty-five economies, found ninety per cent expecting demand for artificial intelligence and data skills to rise, eighty-five per cent prioritising the upskilling of existing staff, and sixty-three per cent naming skills gaps as the principal barrier to transformation.

2.4 Theoretical Framework

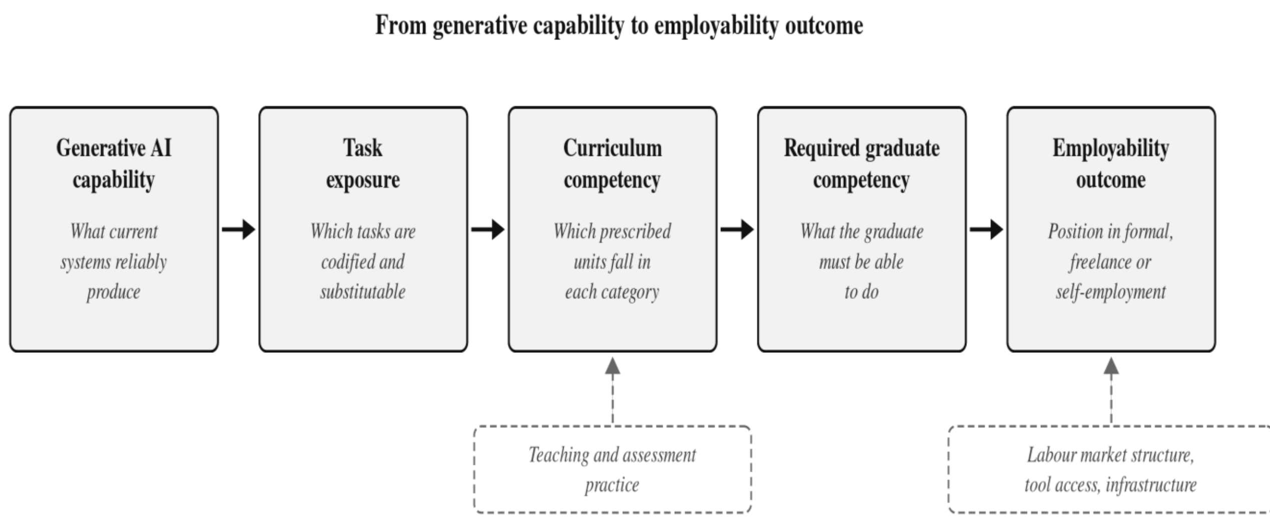
The analysis is grounded in the task-based framework of Autor et al. (2003). Its propositions are that an occupation is a bundle of tasks rather than an indivisible role, that technology substitutes for tasks rather than for workers, and that computer capital substitutes for routine tasks, meaning those expressible in explicit rules, while complementing non-routine problem solving and interactive work.

Applying the framework to generative systems requires one revision. Language models extend substitution beyond the routine to tasks that are non-routine in the original sense yet abundantly represented in public code. Producing a create, read, update and delete endpoint, wiring form validation or manipulating the Document Object Model demand judgement that no explicit rule captures, and are nonetheless generated reliably because many instances exist in training data. The category that predicts substitution is therefore not routineness but codification. This revision generates the rubric applied in Section 2.1.2 and is offered as a theoretical contribution open to test.

The relationships examined above can be represented as a sequence, shown in Figure 1. Generative capability determines which tasks are exposed; task exposure maps onto curriculum competencies; the competencies that survive exposure define what a graduate must be able to do; and that requirement, mediated by local labour market structure, produces an employability outcome. The model is offered as an organising device for the analysis rather than as a validated causal claim, and each transition is a candidate for empirical study.

Figure 1

Proposed model relating generative capability to employability outcome



Note. Developed by the authors. Broken arrows indicate moderating influences that were not measured in this study.

3. FINDINGS AND DISCUSSION

3.1 Curriculum Load and Exposure

Applying the rubric in Table 1 to the ninety-two prescribed credit units produces the distribution in Table 4.

Table 4

Distribution of HND Software and Web Development Credit Units by AI-Exposure Category

Category	Courses	Credit units	% of load
A. Codified implementation	C++ Programming, Python Programming, Database Design I and II, Front End Development I, Back End Development I	18	19.6
B. Foundation and enabling	Operating System, Data Communication and Networks, Computer Architecture, Embedded System Development, Front End Development II,	25	27.2

Category	Courses	Credit units	% of load
	Back End Development II, Advanced Data Structures and Algorithms, Operations Research, Advanced Statistics for Computing		
C. Specification, verification and accountability	Introduction to Software Engineering, Software Design and Architecture, Software Testing and Quality Assurance, Security in Software Development, Project Management, Human Computer Interface, Ethical and Professional Practice, Seminar, Project, Research Methods, Artificial Intelligence, Mandatory Skills Qualification I and II, Entrepreneurship courses, English and Communication courses	49	53.3
Total		92	100.0

Note. Classification and percentages were calculated by the authors from the National Board for Technical Education (2023) HND

Software and Web Development curriculum, applying the rubric in Table 1 to stated course objectives. Percentages express curriculum load only and do not measure labour market exposure, employability value or the relative importance of competencies to employers.

That qualification is essential and bears repetition. The figures state how prescribed instructional load is distributed across three content categories. They do not establish that 19.6 per cent of a graduate's labour market value is at risk, nor that the competencies in Category C command 53.3 per cent of employer demand. A two-unit course may carry greater market weight than a six-unit course, and nothing in the credit allocation speaks to that. What the distribution does establish is narrower and still useful: the codified implementation content on which student anxiety focuses constitutes a minority of prescribed load, and the programme devotes a larger share to content of a kind that the reviewed evidence associates with continuing and possibly rising demand.

The anxiety expressed in programming classes is therefore attached to a real phenomenon but misjudges its scope within the curriculum. What a language model reproduces most reliably is a narrow band of the diploma: the introductory syntax of C++, Python and PHP, elementary Document Object Model manipulation, standard styling and conventional database schemas.

Two further observations qualify the reading. The assessment scheme allocates fifty per cent of marks to practical work (NBTE, 2023), so the codified band occupies more of a student's experience than its credit share suggests. A student who spends most laboratory time producing features by hand may reasonably conclude that feature production is the purpose of the diploma. Second, exposure is not uniform within courses. Back End Development II lists endpoint construction alongside session management, authentication, authorisation, middleware, web tokens, version control and testing (NBTE, 2023). The first is codified; the remainder govern correctness and safety and are where generated code most often fails (Pearce et al., 2022).

3.2 Entry Level Prospects

Evidence on early-career employment supports a differentiated rather than a general contraction. The pattern reported by Brynjolfsson et al. (2025) is consistent with employers withdrawing from work that is codified and supervisable rather than from the occupation itself, while the demand expectations recorded by the World Economic Forum (2025) point to expansion in work combining domain capability with artificial intelligence competence. The two reconcile if the unit of analysis is the task rather than the job, as Autor et al. (2003) propose.

Nigerian conditions differ in ways that alter the reading. Following the methodological revision of 2023, which aligned national measurement with International Labour Organisation practice, the National Bureau of Statistics reported unemployment at 4.3 per cent in the second quarter of 2024, against 33.3 per cent under the previous framework, counting as employed any person of working age engaged in paid work for at least one hour during the reference week (National Bureau of Statistics, 2024). Two accompanying indicators carry more information for present purposes: informal employment stood at 93.0 per cent of employed persons, and the combined measure of unemployment and time-related underemployment stood at 15.3 per cent (National Bureau of Statistics, 2024).

3.2.1 Nigerian Labour Market Conditions

The salient hazard for a Nigerian diplomate is therefore not joblessness as officially counted but absorption into low-value informal work that makes no use of the qualification. Brynjolfsson et al. (2025) describe employers in a deep formal labour market withdrawing from entry-level hiring; Nigeria's formal sector absorbs a small minority of workers, so that mechanism operates on a narrow base. The more consequential question is how artificial intelligence affects the three destinations a diplomate actually reaches.

In formal employment, the binding constraint is plausibly supply rather than demand, and emigration is one mechanism. Bhardwaj and Sharma (2023), synthesising seventy-five studies of cross-border movement among skilled professionals, identify wage differentials, career progression prospects and institutional quality as principal enablers, and argue that consequences for sending economies run in two directions, since remittances, diaspora networks and return migration can transmit capability back. Because foreign employers bid most actively for practitioners who already hold experience, departures concentrate in that group and domestic shortage settles above the entry band. A diplomate able to work at the level of design, verification and integration is positioned to enter that gap. Whether this holds for Nigerian software employment specifically is not established by available data, and the proposition is advanced as an implication of the framework rather than as a measured finding.

In freelance and remote contracting, the finding of Peng et al. (2023) that gains concentrate among less experienced developers applies with force to a diplomate competing for small contracts, and the brain gain channel described by Bhardwaj and Sharma (2023) operates without relocation where a developer resident in Nigeria serves foreign clients. Competitive pressure rises simultaneously, since the same tools reach every bidder, so the distinguishing attribute is demonstrable reliability rather than speed.

In self-employment, if a working first product can be reached with fewer people and less time, the effect should be greater where start-up finance is constrained. No study located here quantifies this for Nigeria, and the point is offered as a reasoned expectation open to test. The curriculum anticipates the path, prescribing six credit units of entrepreneurship alongside a six-unit Project (NBTE, 2023).

Three constraints qualify this reading. Reliable electricity and affordable connectivity remain uneven across institutions and localities, and generative tools are demanding of both. Capable model access is priced in foreign currency, placing the most capable tools beyond many students at prevailing exchange rates and risking the reproduction of existing inequalities within the profession. The workplace exposure deficit identified by Otache (2022) persists, and tool fluency does not substitute for it.

Recommendations that direct students outside the programme are seldom acted upon. The competencies in Table 5 are anchored in prescribed courses, so each represents a reorientation of existing study rather than an addition to it.

3.3 Competencies Graduates Should Acquire

Table 5

Artificial intelligence competencies mapped to curriculum anchors

AI competency	Curriculum anchor	Recommended practice
Specification and decomposition	Software Engineering; Research Methods; Project Management.	Require students to formulate specifications before prompting.
Code comprehension	C++ Programming; Python Programming; Algorithms.	Assess tracing, debugging and explanation of generated code.
AI-code security	Security in Software Development; Back End Development II.	Require vulnerability identification and remediation.
AI-output testing	Software Testing and Quality Assurance.	Require systematic testing of generated code.
AI-system integration	Artificial Intelligence; Back End Development II; Database Design II.	Develop applications integrating authenticated AI services.
Architectural judgement	Software Design and Architecture; Human Computer Interface	Require structural decisions before delegating implementation.

Note: Curriculum anchors identified by the authors from the National Board for Technical Education (2023) HND Software and Web Development curriculum.

The integration competency offers the largest repositioning at the least distance. Back End Development II already prescribes endpoint construction, authentication, authorisation, web tokens and consumption of external interfaces through cURL requests (NBTE, 2023). A student holding those skills is a short step from applications that retrieve from an organisation's own records and pass that material to a model, the pattern surveyed in its more advanced agentic forms by Singh et al. (2025).

Two structural features support this reorientation without curricular amendment. Programme objective seven requires diplomates to obtain industry certification, and the award is conditional on an NBTE-approved certification (NBTE, 2023), so certification choice is a lever already available. The Mandatory Skills Qualification courses, carrying eight credit units of wholly practical work, offer a second vehicle of the same kind.

4. CONCLUSION AND RECOMMENDATIONS

4.1 Conclusion

The question raised in programming classes admits a qualified answer. The available evidence suggests that the HND Software and Web Development programme remains relevant in an AI-assisted development environment, particularly where training emphasises code comprehension, software design, testing, security, system integration and verification. That relevance is conditional rather than automatic, and it rests on how the programme is taught and how students approach it.

Three observations support it. The curriculum devotes just under a fifth of prescribed load to codified implementation content and over half to content concerned with specification, verification, security, communication and accountability. Reviewed evidence indicates that generative assistance redistributes engineering effort rather than removing it, and that quality assurance omitted at generation reappears later as defect and vulnerability (Fawzy et al., 2026; Pearce et al., 2022; Stack Overflow, 2025). Experienced practitioners retain control over design and implementation, drawing on expertise to constrain what agents produce (Huang et al., 2025). Together these suggest that comprehension has moved toward the centre of the occupation, although the study does not establish this causally and no Nigerian labour market data test it.

4.2 Recommendations

The recommendations below are organised by level of responsibility. Those addressed to the regulator are framed as proposals for consideration at scheduled curriculum review rather than as findings about employer requirements, which this study did not measure.

4.2.1 For students

Students on the programme should develop strong code comprehension, treating the programming courses as training in reading and reasoning about code rather than in producing it quickly. They should learn structured prompting, which begins with the ability to write an unambiguous specification. They should build debugging and testing capability deliberately, since the evidence identifies inability to debug as the characteristic weakness of unsupervised generation (Fawzy et al., 2026). They should acquire secure coding competence and apply it specifically to generated output. They should learn to integrate model interfaces into applications over authenticated endpoints. Finally, they should assemble a portfolio that demonstrates AI-assisted development together with evidence of the verification applied to it, since demonstrable reliability rather than speed distinguishes candidates in a market where every competitor holds the same tools.

4.2.2 For polytechnics

Departments should redesign practical assessment within the existing fifty per cent weighting so that a defined share of practical marks, which the authors suggest be set initially at one third and reviewed after one session, requires students to audit, secure, test and justify changes to code they did not write. Lecturers should receive structured development in AI-assisted software development, extending the model already established through the Board's Cisco Academy partnership. Institutions should provide appropriate tooling and the electricity and connectivity it requires, since unequal access will otherwise reproduce existing disadvantage. Departments should introduce AI-assisted code review exercises, in which students critique generated code against stated criteria. Industry partnerships should be strengthened, addressing the workplace exposure deficit that predates the present question (Otache, 2022).

4.2.3 For the National Board for Technical Education

At scheduled curriculum review, the Board may wish to consider periodic revision of learning outcomes for the implementation courses so that comprehension and verification are stated alongside production; incorporation of AI-assisted development competencies within existing course specifications rather than solely within the separate Artificial Intelligence programme; issuance of guidance on responsible use of generative systems in coursework and assessment; and explicit treatment of AI-code security, privacy and verification at the next review of the Security in Software Development and Software Testing and Quality Assurance specifications. Institutional provision of electricity, connectivity and tool access may also warrant consideration as an accreditation resource matter.

4.3 Limitations of the Study

Several limitations qualify the conclusions. The curriculum coding was performed by a single coder against a stated rubric, without independent double coding or an inter-rater reliability statistic, so the classification should be treated as a reproducible proposal rather than a validated instrument. The literature strand was purposive and single-screened. Credit-unit proportions describe instructional load and not labour market value. No Nigerian data disaggregate to this occupation, so international evidence was applied with explicit caution and the propositions drawn from it are offered as implications rather than findings. The study was prompted by student questions but did not survey students, so their own accounts are absent. The capabilities examined change quickly.

4.4 Directions for Future Research

These limitations indicate the work that should follow. An independent expert rating exercise would test the classification and yield a reliability statistic. A survey of students and lecturers across institutions offering the programme would establish patterns of tool use, confidence and career expectation. A tracer study of diplomates would supply the employment evidence Nigeria lacks, and an employer study would establish what firms pay for at entry level, which this study did not measure and on which its recommendations to the regulator are deliberately conditional. The coding method transfers directly to the Cyber Security and Data Protection and the Networking and Cloud Computing streams.

The study contributes a credit-weighted classification of an approved Nigerian technical curriculum against generative capability, together with the rubric that produced it; a refinement of the task-based framework replacing routineness with codification as the predictor of substitution; a reading of graduate prospects fitted to Nigerian labour market structure; and an assessment redesign that reorients practical work toward verification without amending approved content.

REFERENCES

Autor, D. H., Levy, F., & Murnane, R. J. (2003). The skill content of recent technological change: An empirical exploration. *The Quarterly Journal of Economics, 118*(4), 1279–1333. https://doi.org/10.1162/003355303322552801

Becker, B. A., Denny, P., Finnie-Ansley, J., Luxton-Reilly, A., Prather, J., & Santos, E. A. (2023). Programming is hard, or at least it used to be: Educational opportunities and challenges of AI code generation. In *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1* (pp. 500–506). Association for Computing Machinery. https://doi.org/10.1145/3545945.3569759

Becker, J., Rush, N., Barnes, E., & Rein, D. (2025). *Measuring the impact of early-2025 AI on experienced open-source developer productivity* (arXiv:2507.09089). arXiv. https://doi.org/10.48550/arXiv.2507.09089

Bhardwaj, B., & Sharma, D. (2023). Migration of skilled professionals across the border:

Brain drain or brain gain? *European Management Journal, 41*(6), 1021–1033. https://doi.org/10.1016/j.emj.2022.12.011

Brynjolfsson, E., Chandar, B., & Chen, R. (2025). *Canaries in the coal mine? Six facts about the recent employment effects of artificial intelligence* [Working paper]. Stanford Digital Economy Lab. https://digitaleconomy.stanford.edu/publication/canaries-in-the-coal-mine-six-facts-about-the-recent-employment-effects-of-artificial-intelligence/

Denny, P., Prather, J., Becker, B. A., Finnie-Ansley, J., Hellas, A., Leinonen, J., Luxton-Reilly, A., Reeves, B. N., Santos, E. A., & Sarsa, S. (2024). Computing education in the era of generative AI. *Communications of the ACM, 67*(2), 56–67. https://doi.org/10.1145/3624720

Fawzy, A., Tahir, A., & Blincoe, K. (2026). Vibe coding in practice: Motivations, challenges, and a future outlook, a grey literature review. In *Proceedings of the IEEE/ACM 48th International Conference on Software Engineering: Software Engineering in Practice*. Association for Computing Machinery. https://doi.org/10.1145/3786583.3786866

Gama, K., Calegario, F., Jackson, V., Nolte, A., Morais, L. A., & Garcia, V. (2026). "Can you feel the vibes?": An exploration of novice programmer engagement with vibe coding. In *Proceedings of the IEEE/ACM 48th International Conference on Software Engineering: Software Engineering Education and Training*. Association for Computing Machinery. https://doi.org/10.48550/arXiv.2512.02750

Huang, R., Reyna, A., Hempel, B., Lerner, S., & Xia, H. (2025). *Professional software developers don't vibe, they control: AI agent use for coding in 2025* (arXiv:2512.14012). arXiv. https://doi.org/10.48550/arXiv.2512.14012

Karpathy, A. (2025, February 2). *There's a new kind of coding I call "vibe coding"* [Post]. X. https://x.com/karpathy/status/1886192184808149383?s=20

National Board for Technical Education. (2023). *Higher National Diploma (HND) Software and Web Development: Curriculum and course specifications*. National Board for Technical Education.

National Board for Technical Education. (2024, September 2). *NBTE partners with Cisco to train over 500 computer science lecturers on new HND programmes*. https://web.nbte.gov.ng/node/74

National Bureau of Statistics. (2024). *Nigeria labour force survey, Q2 2024*. https://nigerianstat.gov.ng/pdfuploads/NLFS_Q2_2024.pdf

National Bureau of Statistics. (2025). *Nigerian gross domestic product report, Q2 2025*. National Bureau of Statistics.

Otache, I. (2022). Enhancing graduates' employability through polytechnic–industry collaboration. *Industry and Higher Education, 36*(4), 470–478. https://doi.org/10.1177/09504222211063140

Pearce, H., Ahmad, B., Tan, B., Dolan-Gavitt, B., & Karri, R. (2022). Asleep at the keyboard? Assessing the security of GitHub Copilot's code contributions. In *2022 IEEE Symposium on Security and Privacy (SP)* (pp. 754–768). IEEE. https://doi.org/10.1109/SP46214.2022.9833571

Peng, S., Kalliamvakou, E., Cihon, P., & Demirer, M. (2023). *The impact of AI on developer productivity: Evidence from GitHub Copilot* (arXiv:2302.06590). arXiv.

https://doi.org/10.48550/arXiv.2302.06590

Prather, J., Denny, P., Leinonen, J., Becker, B. A., Albluwi, I., Craig, M., Keuning, H., Kiesler, N., Kohn, T., Luxton-Reilly, A., MacNeil, S., Petersen, A., Pettit, R., Reeves, B. N., & Savelka, J. (2023). The robots are here: Navigating the generative AI revolution in computing education. In *2023 Working Group Reports on Innovation and Technology in Computer Science Education* (pp. 108–159). Association for Computing Machinery. https://doi.org/10.1145/3623762.3633499

Sarkar, A., & Drosos, I. (2025). Vibe coding: Programming through conversation with artificial intelligence. In *Proceedings of the 36th Annual Conference of the Psychology of Programming Interest Group*. Psychology of Programming Interest Group. https://doi.org/10.48550/arXiv.2506.23253

Singh, A., Ehtesham, A., Kumar, S., & Talaei Khoei, T. (2025). *Agentic retrieval-augmented generation: A survey on agentic RAG* (arXiv:2501.09136). arXiv. https://doi.org/10.48550/arXiv.2501.09136

Stack Overflow. (2025). *2025 developer survey*. https://survey.stackoverflow.co/2025/

World Economic Forum. (2025). *Future of jobs report 2025*. World Economic Forum. https://www.weforum.org/publications/the-future-of-jobs-report-2025/

GENERATIVE AI AND THE FUTURE OF HIGHER EDUCATION: RETHINKING ASSESSMENT, ACADEMIC INTEGRITY, AND DIGITAL PEDAGOGY IN NIGERIAN TERTIARY INSTITUTIONS

AYODELE, Oluwakemi Sade[1], OYELOLA Emmanuel[2]

[1]Department of Computer Science

Kogi State Polytechnic, Lokoja

[2]Department of Library and Information Science
Kogi State Polytechnic, Lokoja

Abstract

The rapid emergence of Generative Artificial Intelligence (GenAI) has created significant opportunities and challenges for higher education globally. Tools such as ChatGPT, Gemini, Claude and other large language model applications can generate text, explain concepts, write computer code, summarise information, translate content, provide feedback and support research activities. While these capabilities offer opportunities for personalised learning, improved teaching efficiency and enhanced access to educational resources, they have simultaneously raised concerns regarding academic integrity, assessment validity, student dependency, misinformation, data privacy and the changing role of educators. These challenges are particularly significant for Nigerian tertiary institutions, where digital transformation is occurring alongside persistent challenges relating to infrastructure, digital literacy, unequal access to technology and institutional capacity. This paper examines the implications of Generative AI for assessment, academic integrity and digital pedagogy in Nigerian tertiary institutions. An integrative literature review methodology was adopted to synthesise scholarly publications, policy documents and authoritative reports on Generative AI and higher education. The review indicates that traditional assessment approaches based primarily on take-home essays, unsupervised assignments and conventional online submissions are increasingly vulnerable to AI-assisted production. However, banning GenAI is unlikely to provide a sustainable solution. The paper argues for a transition from AI-resistant education to AI-aware and AI-augmented education. It proposes a human-centred framework built around AI literacy, redesigned assessment, transparent AI-use policies, continuous assessment, authentic learning, oral and process-based evaluation, faculty development, data protection and equitable access. The paper concludes that Nigerian tertiary institutions should strategically integrate GenAI into teaching and learning while preserving human agency, critical thinking, creativity, ethical reasoning and academic integrity.

Keywords**:** Generative Artificial Intelligence, higher education, academic integrity, assessment, digital pedagogy, ChatGPT, Nigerian tertiary institutions, AI literacy

1. INTRODUCTION

Artificial Intelligence (AI) has evolved from a specialised computing technology into a transformative force affecting virtually every sector of society. In education, the emergence of Generative Artificial Intelligence (GenAI) represents one of the most significant technological developments of recent years. Unlike earlier educational technologies that primarily provided access to information or facilitated communication, GenAI systems can generate human-like text, images, computer code, audio and other forms of content in response to natural-language prompts. The public release of ChatGPT in late 2022 accelerated global interest in the educational implications of these technologies (UNESCO, 2023).

Generative AI has rapidly entered higher education environments. Students use AI tools for brainstorming, summarising academic materials, explaining difficult concepts, improving writing, translating texts, generating computer code and obtaining feedback. Academic staff can also use these technologies to develop lesson plans, generate examples, create assessment questions, provide formative feedback and support administrative activities. A systematic review by Baig and Yadegaridehkordi (2024) found that ChatGPT applications in higher education are expanding across activities involving students, academic staff, researchers and administrative personnel.

The educational value of GenAI, however, is accompanied by serious concerns. One of the most prominent is academic integrity. Students can use generative AI to produce essays, reports, programming solutions and responses to examination questions with limited evidence of their own intellectual contribution. Consequently, traditional assessment methods may no longer reliably demonstrate what students know or can do. A 2024 study involving 337 university students found that more than one-third had used chatbots to assist with assessments, while some students did not necessarily consider such use a breach of academic integrity (Bittle & El-Gayar, 2024). This finding highlights an important distinction between AI use and AI misuse.

The challenge therefore extends beyond detecting AI-generated content. It concerns the fundamental purpose of assessment. If an assessment is designed merely to test a student's ability to produce a polished essay, and a generative AI system can produce such an essay within seconds, the assessment may no longer adequately measure the intended learning outcome. Higher education institutions consequently need to reconsider what should be assessed, how it should be assessed and what constitutes legitimate assistance from AI.

UNESCO (2023) argues for a human-centred approach to GenAI in education, emphasising human agency, inclusion, equity, cultural and linguistic diversity, privacy and ethical use. UNESCO also notes that educational institutions need appropriate policies and capacity development to respond to GenAI rather than simply reacting to the technology after it has already become embedded in educational practice.

The Nigerian higher education system cannot remain outside this global transformation. Universities, polytechnics and colleges of education increasingly operate within digital learning environments, and students have access to publicly available AI tools through smartphones and computers. At the same time, Nigerian tertiary institutions face contextual challenges including unequal internet access, inadequate digital infrastructure, limited institutional AI policies, varying levels of digital literacy among lecturers and students, and concerns regarding data protection (Ayodele et al,, 2023).

The central argument of this paper is that Generative AI should neither be treated exclusively as an academic threat nor accepted uncritically as an educational solution. Rather, Nigerian tertiary institutions should develop a balanced approach in which AI becomes a tool for enhancing learning while human judgement remains central to assessment, scholarship and academic decision-making.

1.1 Statement of the Problem

The rapid adoption of GenAI has created a mismatch between emerging technological capabilities and existing educational practices. Many conventional assessment methods were designed before students had access to AI systems capable of generating coherent essays, solving problems and producing computer programs.

The problem is therefore not simply that students may use AI to cheat. A deeper problem is that institutions may continue to use assessment models that make inappropriate AI use easy and authentic learning difficult to verify.

Academic integrity is further complicated by the absence of universally accepted definitions of permissible and impermissible AI use. For example, using an AI system to generate ideas, correct grammar or explain a difficult concept may constitute legitimate learning support in one institution but be prohibited in another. Research involving 2,555 students at the University of Liverpool found substantial student awareness and use of generative AI, while 41.1% believed that universities should have institution-wide policies defining when AI technologies are appropriate (Johnston et al., 2024).

For Nigerian tertiary institutions, this uncertainty creates challenges for students, lecturers, examination officers, quality assurance units and institutional management. There is therefore a need for a systematic reconsideration of assessment, academic integrity and digital pedagogy within the context of GenAI.

1.2 Objectives of the Study

The objectives of this paper are to:

1. examine the emerging role of Generative AI in higher education;
2. examine the implications of GenAI for assessment practices in Nigerian tertiary institutions;
3. analyse the implications of GenAI for academic integrity;
4. explore opportunities for integrating GenAI into digital pedagogy;
5. identify challenges associated with GenAI adoption in Nigerian tertiary institutions; and
6. propose a human-centred framework for responsible GenAI integration into Nigerian higher education.

1.3 Research Questions

The paper addresses the following questions:

1. How is Generative AI transforming teaching and learning in higher education?
2. What challenges does GenAI present to conventional assessment practices?
3. How does GenAI affect academic integrity in tertiary education?
4. What opportunities does GenAI provide for digital pedagogy?
5. How can Nigerian tertiary institutions integrate GenAI while protecting academic integrity and human-centred learning?

2. LITERATURE REVIEW

2.1 Concept of Generative Artificial Intelligence

Generative Artificial Intelligence refers to AI systems capable of producing new content based on patterns learned from large datasets. Large Language Models (LLMs), which underpin many contemporary GenAI applications, can generate text and perform tasks such as summarisation, question answering, translation, coding assistance and content transformation.

The educational significance of GenAI arises from its ability to interact with users through natural language. Instead of requiring users to learn specialised software interfaces, students can communicate with AI systems using ordinary language. This makes GenAI highly accessible and potentially valuable as an educational assistant.

However, GenAI does not function as a human teacher or expert. AI-generated outputs can contain inaccurate information, fabricated references, biased interpretations and misleading explanations. Consequently, students require sufficient AI literacy to critically evaluate AI-generated information rather than accepting it automatically.

UNESCO (2023) emphasises that GenAI should support, rather than replace, human agency in education. Its guidance identifies issues involving privacy, equity, inclusion, cultural diversity, ethics and the need for appropriate institutional regulation.

2.2 Generative AI and Higher Education

The impact of GenAI on higher education is multidimensional. It affects teaching, learning, assessment, research, student support and academic administration.

Dempere et al. (2023), in a systematic review of ChatGPT's impact on higher education, identified both educational opportunities and concerns associated with the technology.

Potential educational applications include:

i. personalised explanations of difficult concepts;
ii. automated formative feedback;
iii. generation of practice questions;
iv. language support;
v. tutoring and academic assistance;
vi. brainstorming and idea generation;
vii. programming and debugging assistance;
viii. research support;
ix. lesson and course material development; and
x. administrative assistance.

The literature therefore suggests that the educational value of GenAI extends beyond student essay writing. The technology can potentially support a more personalised and interactive learning environment.

However, its effectiveness depends on how it is integrated into pedagogy. Merely giving students access to AI tools does not automatically produce better learning outcomes. Overdependence may reduce opportunities for students to struggle productively with complex problems, develop independent reasoning or construct knowledge through direct experience.

UNESCO (2023) cautions that excessive reliance on AI-generated information may reduce opportunities for learners to develop knowledge through experimentation, direct experience and collaborative learning.

2.3 Generative AI and Assessment

Assessment is arguably the area of higher education most directly disrupted by GenAI.

Traditional assessment practices frequently include essays, take-home assignments, reports, programming exercises and online quizzes. These methods often assume that the submitted product is primarily generated by the student. GenAI challenges this assumption.

A student can now use an AI tool to generate an essay, improve the structure of a report, solve a programming task or formulate answers to theoretical questions. Consequently, the final submitted product may provide insufficient evidence of the student's actual knowledge and skills.

Recent research on higher education assessment in the era of GenAI argues that assessment practices need to evolve in response to the capabilities of these tools. Some forms of assessment can be completed effectively by GenAI, while others expose limitations in AI-generated responses and therefore remain valuable when appropriately designed (Ogunleye et al., 2024).

Similarly, a systematic review of automated assessment systems found substantial potential for AI-supported assessment and feedback, while emphasising the importance of evaluating educational outcomes and human-centred applications (Zhai et al., 2024).

The issue is therefore not whether AI should be present in assessment, but how assessment can be redesigned so that students demonstrate authentic knowledge, skills and competencies.

2.4 Academic Integrity in the Age of GenAI

Academic integrity refers to principles and practices associated with honesty, responsibility, fairness, trust and ethical conduct in academic work. Traditional forms of academic misconduct include plagiarism, fabrication, falsification, examination malpractice and unauthorised collaboration.

GenAI introduces a new dimension because the content may not be copied directly from another human author. Instead, it may be generated by an AI system. This complicates conventional definitions of plagiarism.

A systematic literature review covering academic integrity violations from 2013 to 2023 identified individual, institutional, social, cultural and technological factors influencing academic misconduct and highlighted the need for multifaceted institutional responses in the AI era.

The most important issue is therefore not merely whether AI-generated content can be detected. Detection technologies themselves have limitations, and false positives can create serious consequences for students. Institutions should avoid relying exclusively on AI detectors to establish misconduct.

Instead, academic integrity policies should define acceptable AI use explicitly. Students should know whether they may use AI for brainstorming, grammar correction, translation, coding assistance, literature discovery, feedback or other activities. Where AI is permitted, appropriate acknowledgement or disclosure should be required.

2.5 Generative AI and Digital Pedagogy

Digital pedagogy refers to the integration of digital technologies into teaching and learning in ways that support educational objectives. GenAI creates opportunities to move from conventional technology-supported learning toward more interactive and personalised learning experiences.

Lecturers can use GenAI to generate alternative explanations of complex concepts, create differentiated learning materials, develop case studies, formulate practice questions and provide initial feedback. Students can use AI as a learning companion to ask questions, obtain explanations and explore alternative perspectives.

However, digital pedagogy should not become "AI pedagogy" in which the technology becomes the centre of the learning process. The lecturer remains responsible for curriculum design, intellectual judgement, ethical guidance and verification of knowledge.

Research on student perspectives indicates that students themselves recognise the need for clearer institutional guidance. Johnston et al. (2024) found substantial support for some forms of AI assistance but much less support for students using ChatGPT to write an entire essay.

This suggests that students may not necessarily be seeking unrestricted AI use. Rather, many need clear boundaries distinguishing acceptable assistance from academic misconduct.

2.6 Opportunities for Nigerian Tertiary Institutions

For Nigerian tertiary institutions, GenAI could contribute to:

Personalised learning

AI systems can provide explanations according to individual learning needs and levels of understanding.

Improved access to learning resources

Students can interact with AI systems at any time, potentially supplementing limited access to lecturers and physical learning resources.

Lecturer productivity

Lecturers can use AI to generate preliminary lesson plans, examples, quizzes and other instructional resources, subject to human verification.

Support for students with language challenges

GenAI can assist with grammar, translation and comprehension, potentially supporting students who struggle with academic English.

Research support

AI tools can support brainstorming, coding, data interpretation and literature exploration, although researchers must verify sources and maintain research integrity.

Development of AI literacy

Responsible use of GenAI can prepare graduates for workplaces in which AI is increasingly becoming part of professional practice.

2.7 Challenges of GenAI Adoption in Nigeria

Despite these opportunities, several challenges require attention.

Digital inequality

Not all students have equal access to reliable internet connectivity, computers, smartphones or paid AI services. Unregulated AI integration could therefore widen existing educational inequalities.

Infrastructure

Reliable electricity, internet connectivity, institutional learning management systems and appropriate computing infrastructure remain important requirements for digital education.

Staff capacity

Lecturers require training not only in operating AI tools but also in prompt design, AI evaluation, assessment redesign, ethics and data protection.

Academic integrity

Institutions must develop clear rules governing legitimate and illegitimate AI use.

Data privacy

Students and staff may inadvertently submit personal, confidential or institutional information to external AI systems. UNESCO identifies data privacy as a major issue requiring institutional safeguards.

Misinformation and hallucination

AI-generated content may sound authoritative while being factually incorrect. Students therefore require critical AI literacy.

Overdependence

Excessive reliance on AI may weaken independent thinking, creativity, writing ability and problem-solving skills.

3. METHODOLOGY

3.1 Research Design

This study adopted an integrative literature review design. The approach was considered appropriate because the objective was to synthesise existing knowledge concerning Generative AI, assessment, academic integrity and digital pedagogy rather than collect primary data from students or lecturers.

The review focused particularly on literature relevant to higher education and the implications for Nigerian tertiary institutions.

3.2 Sources of Data

Relevant literature was identified from scholarly and authoritative sources, including:

i. peer-reviewed journal articles;
ii. systematic literature reviews;
iii. academic conference publications;
iv. UNESCO reports and policy guidance;
v. higher education policy documents; and

vi. relevant scholarly publications on AI, assessment and academic integrity.

Priority was given to recent literature published from 2023 onward because of the rapid development of GenAI following the emergence of ChatGPT.

3.3 Inclusion Criteria

Literature was considered relevant where it:

1. addressed Generative AI, ChatGPT, LLMs or related AI technologies;
2. focused on higher or tertiary education;
3. addressed assessment, academic integrity, teaching, learning or digital pedagogy;
4. contained implications relevant to educational policy or practice; and
5. provided sufficient information for thematic synthesis.

3.4 Data Analysis

The selected literature was analysed thematically. Four major themes emerged:

1. Transformation of assessment
2. Academic integrity and ethical AI use
3. Transformation of digital pedagogy
4. Institutional readiness and policy requirements

The findings were interpreted within the Nigerian tertiary education context.

3.5 Scope and Limitation

The study is conceptual and literature-based. It does not claim to provide statistical evidence concerning the prevalence of GenAI use among Nigerian tertiary institution students. Consequently, the findings should be interpreted as a synthesis of existing evidence and a framework for institutional practice rather than as results from a Nigerian field survey.

4. RESULTS AND DISCUSSION

4.1 Theme One: Traditional Assessment Requires Redesign

The review indicates that GenAI is making some conventional assessment practices increasingly vulnerable. Essays, take-home assignments and unsupervised online tasks can potentially be generated or substantially assisted by AI.

This does not mean that essays and written assignments should be abandoned. Rather, their design should change.

Assessment should increasingly focus on:

i. the process of learning;
ii. application of knowledge;
iii. critical analysis;
iv. problem-solving;
v. reflection;
vi. originality of ideas;
vii. practical demonstrations;

viii. oral defence; and

ix. authentic real-world tasks.

For example, instead of asking a student to "Write an essay on cybersecurity," an institution could require the student to analyse a specific cybersecurity incident, document the research process, explain the decisions made, present the work orally and respond to questions from the lecturer.

This type of assessment makes it substantially more difficult to outsource the entire learning process to an AI system.

Proposed Assessment Transformation

Traditional Assessment	AI-Aware Assessment
One final essay	Progressive research portfolio
Take-home assignment	Assignment + oral defence
Generic questions	Context-specific problems
Product-focused	Process-and-product focused
Unsupervised writing	Supervised and reflective components
Recall-based questions	Application and analysis
AI prohibition	Clearly defined AI-use rules
Final examination only	Continuous and authentic assessment

The implication is that assessment should move from asking "What answer can the student produce?" to asking "What can the student demonstrate, explain, apply and defend?"

4.2 Theme Two: Academic Integrity Should Shift from Detection to Responsible Use

The literature indicates that institutions cannot depend exclusively on AI detection technologies. The rapidly evolving nature of GenAI means that detection mechanisms may become less reliable as models improve.

A more sustainable strategy is to develop a culture of responsible AI use.

Students should be taught:

i. what GenAI is;

ii. how it produces outputs;

iii. its limitations;

iv. how hallucinations occur;

v. how to verify AI-generated information;

vi. when AI use is permissible;

vii. how to disclose AI assistance; and

viii. why submitting AI-generated work as one's own may constitute academic misconduct.

Academic integrity policies should therefore distinguish between AI-assisted learning and AI-substituted learning.

For example, using AI to explain a difficult programming concept may support learning. Asking AI to generate an entire programming assignment and submitting it without understanding or acknowledgement undermines the learning objective.

This distinction is important because evidence suggests that students themselves do not necessarily regard all AI use as equivalent to cheating. Bittle and El-Gayar (2024) found that some students who used chatbots for assessments did not perceive such use as a breach of academic integrity.

Consequently, institutions must communicate clear, consistent and understandable policies.

4.3 Theme Three: GenAI Should Be Integrated into Digital Pedagogy

The review demonstrates that GenAI can provide valuable pedagogical support when appropriately integrated.

A lecturer could, for example, ask students to:

1. generate an AI response to a question;
2. identify inaccuracies or weaknesses in the response;
3. compare the response with scholarly sources;
4. improve the answer;
5. explain the changes they made; and
6. reflect on what they learned.

This transforms AI from a shortcut into an object of critical inquiry.

For Computer Science education, students could be asked to use AI-generated code as a starting point, test the code, identify security vulnerabilities, debug it and explain the final solution.

For social sciences, students could critically analyse AI-generated arguments and identify assumptions, biases and unsupported claims.

For sciences, students could evaluate AI-generated explanations against experimental evidence.

Therefore, the appropriate question is not:

"How do we prevent students from using AI?"

but rather:

"How do we design learning experiences in which students must think critically about AI?"

4.4 Theme Four: The Role of the Lecturer Will Change

GenAI does not necessarily make lecturers less important. Instead, it changes the nature of their work.

The lecturer's role is likely to shift from being primarily a transmitter of information to becoming:

i. a learning designer;
ii. facilitator;
iii. mentor;
iv. evaluator;
v. critical-thinking coach;
vi. AI literacy educator; and
vii. ethical guide.

AI may generate information, but lecturers remain responsible for determining whether that information is educationally appropriate, accurate and relevant to the curriculum.

This shift requires significant professional development. Institutions should establish regular training programmes that expose lecturers to practical AI applications and associated risks.

4.5 Theme Five: Institutional AI Policies Are Essential

A major finding from the literature is the need for clear institutional policies. UNESCO reported that, in a global survey conducted in 2023, fewer than 10% of surveyed schools and universities had formal guidance concerning generative AI.

Although the situation has evolved since that survey, the finding demonstrates the initial gap between technological development and institutional preparedness.

A Nigerian tertiary institution's AI policy should address:

1. acceptable AI use;
2. prohibited AI use;
3. disclosure requirements;
4. citation and acknowledgement of AI assistance;
5. assessment-specific rules;
6. data privacy;
7. research ethics;
8. intellectual property;
9. staff responsibilities;
10. student responsibilities;
11. disciplinary procedures; and
12. periodic policy review.

The policy should not simply state that "ChatGPT is prohibited." Such a rule is increasingly difficult to enforce and may prevent students from developing responsible AI competencies required in the workplace.

4.6 Theme Six: AI Literacy Should Become a Core Graduate Competency

The emergence of GenAI creates a new educational requirement: AI literacy.

AI literacy should include the ability to:

i. understand basic AI concepts;
ii. formulate effective prompts;
iii. evaluate AI-generated content;
iv. identify hallucinations and misinformation;
v. recognise bias;
vi. protect personal and confidential data;
vii. understand intellectual property;
viii. disclose AI assistance appropriately;
ix. use AI ethically; and
x. critically determine when AI should or should not be used.

AI literacy should not be limited to Computer Science students. Students in education, management, social sciences, engineering, health-related disciplines, agriculture and the humanities will increasingly encounter AI in professional environments.

Therefore, Nigerian tertiary institutions should consider incorporating AI literacy into general studies, digital literacy programmes and discipline-specific curricula.

4.7 Proposed Human-Centred GenAI Integration Framework

Based on the literature reviewed, this paper proposes the Human-Centred Generative AI Higher Education Framework (HC-GAI-HEF).

The framework consists of six interconnected pillars:

Pillar 1: Governance

Institutions should establish clear AI policies, ethical guidelines and accountability structures.

Pillar 2: AI Literacy

Students and lecturers should be trained to understand, evaluate and responsibly use GenAI.

Pillar 3: Assessment Transformation

Assessment should emphasise authentic tasks, critical thinking, oral defence, practical demonstrations, portfolios and learning processes.

Pillar 4: Digital Pedagogy

GenAI should be incorporated into teaching activities where it improves learning outcomes without replacing human intellectual engagement.

Pillar 5: Data Protection and Equity

Institutions should protect personal and institutional information while ensuring that unequal access to AI does not widen educational inequality.

Pillar 6: Continuous Evaluation

AI policies and pedagogical practices should be reviewed regularly because AI technologies are evolving rapidly.

The framework can be represented conceptually as:

Governance → AI Literacy → Assessment Transformation → Digital Pedagogy → Equity & Data Protection → Continuous Evaluation

At the centre of the framework is Human Agency, because technology should serve educational objectives rather than determine them.

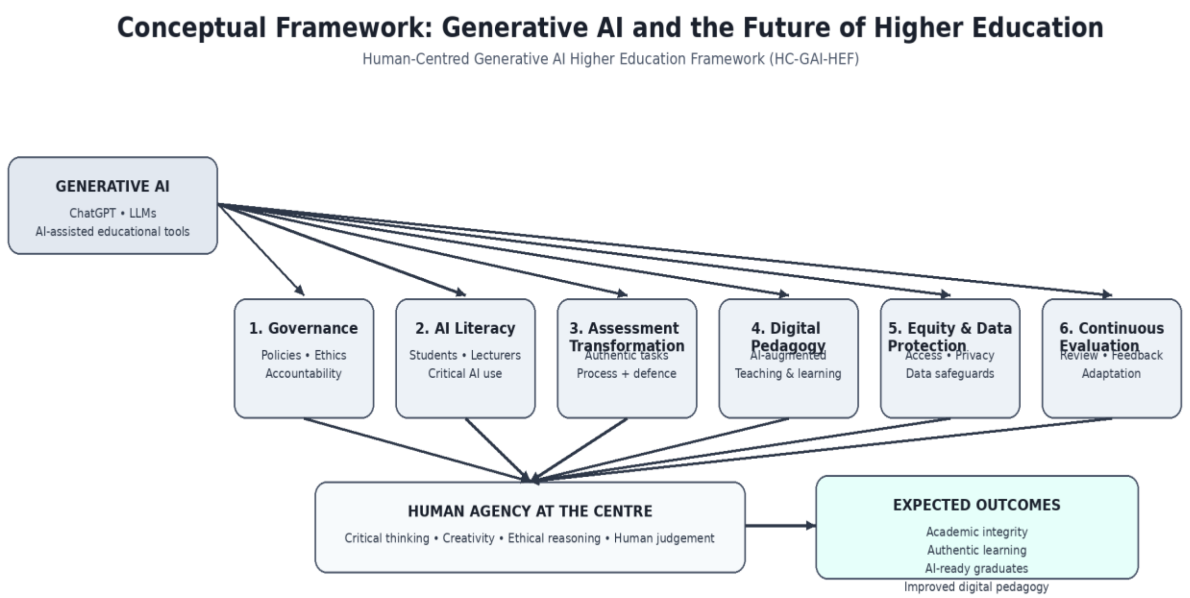


Figure 4.1: Authors' Conceptualisation based on the literature reviewed in this study

4.8 Implications for Nigerian Tertiary Institutions

The findings have several implications for universities, polytechnics and colleges of education in Nigeria.

First, institutions need to acknowledge that GenAI is already part of the educational environment. A policy of complete denial is unlikely to be sustainable.

Second, assessment committees should review existing assessment formats and identify tasks that can easily be completed by AI without meaningful student engagement.

Third, lecturers should receive structured professional development in GenAI.

Fourth, institutions should establish clear AI-use policies that are communicated to students at the beginning of every academic session.

Fifth, Nigerian institutions should pay particular attention to data protection. Students and staff should not be encouraged to upload confidential student records, examination materials, unpublished research or sensitive institutional information into public AI platforms.

Finally, AI adoption must consider the Nigerian digital divide. Institutions should avoid developing AI-dependent educational models that disadvantage students with limited access to connectivity or advanced digital tools.

5. CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

Generative Artificial Intelligence is fundamentally changing the higher education landscape. Its ability to generate text, code, explanations and other forms of content creates significant opportunities for teaching, learning, research and academic support. At the same time, it challenges assumptions underlying conventional assessment and academic integrity.

The central challenge facing Nigerian tertiary institutions is not simply how to prevent students from using AI. It is how to ensure that AI use contributes to genuine learning rather than replacing the intellectual work students are expected to perform.

The literature reviewed indicates that traditional assessment models based heavily on unsupervised essays, take-home assignments and generic online tasks are increasingly vulnerable to GenAI. Consequently, higher education institutions need to rethink assessment around authentic learning, critical thinking, problem-solving, reflection, practical demonstration and oral defence.

Academic integrity policies must also evolve. Rather than focusing exclusively on AI detection, institutions should establish transparent rules for acceptable and unacceptable AI use. Students should be taught how to use GenAI ethically and critically.

For Nigerian tertiary institutions, the adoption of GenAI should be human-centred, equitable, ethical and context-sensitive. GenAI should augment lecturers rather than replace them, support students rather than substitute for their intellectual development, and strengthen rather than weaken academic standards.

The future of higher education is therefore unlikely to be AI versus human education. The more appropriate future is human intelligence enhanced by responsible artificial intelligence.

5.2 Recommendations

Based on the findings, the following recommendations are proposed:

1. Development of institutional GenAI policies

Every Nigerian tertiary institution should develop a comprehensive Generative AI policy covering teaching, learning, assessment, research, academic integrity, data protection and ethical use.

2. Redesign of assessment

Institutions should gradually reduce excessive dependence on generic take-home assignments and introduce authentic, contextualised, process-based and oral assessment components.

3. Introduction of AI literacy programmes

AI literacy should be incorporated into student orientation programmes, general studies courses and discipline-specific curricula.

4. Continuous professional development for lecturers

Institutions should organise regular training for academic staff on GenAI tools, prompt engineering, AI ethics, assessment redesign, fact verification and responsible AI integration.

5. Clear AI disclosure requirements

Where AI use is permitted, students should be required to disclose the nature and extent of AI assistance in their academic work.

6. Human-centred assessment

Assessment should prioritise competencies that require human judgement, creativity, ethical reasoning, contextual understanding, practical skills and critical thinking.

7. Responsible use of AI detection tools

AI detectors should not be treated as definitive evidence of academic misconduct. Any allegation of AI-related misconduct should involve appropriate human review and supporting evidence.

8. Protection of personal and institutional data

Institutions should establish clear guidelines preventing students and staff from entering confidential information, examination materials, personal data or sensitive research information into public AI platforms.

9. Promote equitable access

Institutions should consider the digital divide when integrating GenAI into teaching and assessment. AI-supported education should not create a new category of disadvantaged students.

10. Establish AI innovation and research centres

Nigerian tertiary institutions should establish interdisciplinary AI innovation centres or laboratories to investigate responsible applications of GenAI in education and other sectors.

11. Encourage AI-assisted but human-led research

Researchers should be permitted to use GenAI for appropriate research-support activities while maintaining human responsibility for research design, analysis, interpretation, authorship and scholarly integrity.

12. Continuous review of AI policies

Because GenAI technologies are evolving rapidly, institutional policies should be reviewed periodically rather than treated as permanent documents.

In conclusion, Nigerian tertiary institutions should not wait for Generative AI to disappear or become fully predictable before responding. The technology is evolving too rapidly for that approach. Instead, institutions should develop the capacity to understand it, regulate it, teach with it, teach about it, and critically evaluate its educational consequences.

References

Ayodele, O. S., Aliu, J., Owoeye, F. O., Ajayi, E. A., & Sheidu, A. Y. (2023). The role of artificial intelligence in curriculum development and management. Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology, 11(1), 37–46. https://doi.org/10.22624/AIMS/DIGITAL/V11N2P4.

Baig, M. I., & Yadegaridehkordi, E. (2024). ChatGPT in the higher education: A systematic literature review and research challenges. *International Journal of Educational Research, 127*,102411. https://doi.org/10.1016/j.ijer.2024.102411

Bittle, K., & El-Gayar, O. (2024). The rapid rise of generative AI and its implications for academic integrity: Students' perceptions and use of chatbots for assistance with assessments. *Computers and Education: Artificial Intelligence, 7*,100273. https://doi.org/10.1016/j.caeai.2024.100273

Dempere, J., Modugu, K., Hesham, A., & Ramasamy, L. K. (2023). The impact of ChatGPT on higher education. *Frontiers in Education, 8*, 1206936. https://doi.org/10.3389/feduc.2023.1206936

Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., Baabdullah, A. M., Koohang, A., Raghavan, V., Ahuja, M., Albanna, H., Albashrawi, M. A., Al-Busaidi, A. S., Balakrishnan, J., Barlette, Y., Basu, S., Bose, I., Brooks, L., Buhalis, D., ... Wright, R. (2023). Opinion paper: "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management, 71*, 102642. https://doi.org/10.1016/j.ijinfomgt.2023.102642

Johnston, H., Wells, R. F., Shanks, E. M., Boey, T., & Parsons, B. N. (2024). Student perspectives on the use of generative artificial intelligence technologies in higher education. *International Journal for Educational Integrity, 20*, Article 2. https://doi.org/10.1007/s40979-024-00149-4

Miao, F., & Holmes, W. (2023). *Guidance for generative AI in education and research*. UNESCO.

Ogunleye, B., Zakariyyah, K. I., Ajao, O., Olayinka, O., & Sharma, H. (2024). Higher education assessment practice in the era of generative AI tools. *arXiv*. https://doi.org/10.48550/arXiv.2404.01036

Tlili, A., Shehata, B., Adarkwah, M. A., Bozkurt, A., Hickey, D. T., Huang, R., & Agyemang, B. (2023). What if the devil is my guardian angel: ChatGPT as a case study of using chatbots in education. *Smart Learning Environments, 10*, Article 15. https://doi.org/10.1186/s40561-023-00237-x

UNESCO. (2023). *Guidance for generative AI in education and research*. UNESCO.

Zhai, X., Yin, Y., & others. (2024). Automatic assessment of text-based responses in post-secondary education: A systematic review. *Computers and Education: Artificial Intelligence, 6*, 100206. https://doi.org/10.1016/j.caeai.2024.100206

Zawacki-Richter, O., Marín, V. I., Bond, M., & Gouverneur, F. (2019). Systematic review of research on artificial intelligence applications in higher education—Where are the educators? *International Journal of Educational Technology in Higher Education, 16*, Article 39. https://doi.org/10.1186/s41239-019-0171-0

CYBERSECURITY IN NIGERIAN TERTIARY INSTITUTIONS: STRENGTHENING CYBER RESILIENCE, DATA PROTECTION, AND DIGITAL TRUST IN THE ERA OF DIGITAL TRANSFORMATION

AYODELE, Oluwakemi Sade[1], OYELOLA Emmanuel[2], Halimat Ahuoiza Zubair[1]

[1]Department of Computer Science

Kogi State Polytechnic, Lokoja

[2]Department of Library and Information Science
Kogi State Polytechnic, Lokoja

Abstract

The rapid digital transformation of tertiary education has significantly changed the way universities, polytechnics, and colleges of education in Nigeria deliver teaching, conduct research, manage student records, administer examinations, and provide institutional services. Learning management systems, cloud computing, online registration platforms, electronic payment systems, mobile applications, institutional portals, and digital communication platforms have improved accessibility and operational efficiency. However, increased digital dependence has simultaneously expanded the cyber-attack surface of tertiary institutions. Cyber threats such as phishing, ransomware, credential theft, social engineering, malware, insider threats, data breaches, and denial-of-service attacks pose significant risks to institutional information assets and digital services. The protection of student records, staff information, examination materials, financial information, research data, and intellectual property has therefore become an essential component of educational governance. This paper examines cybersecurity in Nigerian tertiary institutions, with particular emphasis on cyber resilience, data protection, and digital trust. An integrative literature review methodology was adopted to synthesise scholarly publications, cybersecurity frameworks, Nigerian regulatory documents, and authoritative reports. The review identified five major areas requiring institutional attention: cybersecurity governance, human-centred security awareness, technical protection, data protection and privacy, and incident response and recovery. The paper argues that cybersecurity should no longer be treated solely as an Information Technology function but as an institutional governance and risk-management responsibility. A Cyber-Resilient Tertiary Institution Framework (CR-TIF) is proposed, comprising governance and policy, people and awareness, technology and infrastructure, data protection, incident response, and continuous improvement. The paper recommends the development of institution-wide cybersecurity policies, regular security awareness programmes, multifactor authentication, data classification, vulnerability management, incident-response plans, cybersecurity curricula, periodic security audits, and stronger collaboration among tertiary institutions, regulators, cybersecurity professionals, and industry. Strengthening cybersecurity will not only protect institutional assets but also enhance confidence, continuity, privacy, and digital trust within Nigerian higher education.

Keywords: Cybersecurity, cyber resilience, data protection, digital trust, tertiary institutions, Nigerian higher education, information security, cyber threats

1. INTRODUCTION

Digital transformation has become an increasingly important component of contemporary higher education. Nigerian universities, polytechnics, and colleges of education are progressively adopting digital technologies to support teaching, learning, research, communication, student administration, electronic payments, examination management, and institutional decision-making. This transformation creates significant opportunities for improving educational access and institutional efficiency, but it also increases institutional dependence on digital infrastructure and consequently expands the potential attack surface for cyber threats (Zawacki-Richter et al., 2019; World Economic Forum, 2024).

Cybersecurity refers broadly to the technologies, processes, policies, and practices used to protect information systems, networks, devices, applications, and data against unauthorised access, disruption, modification, disclosure, or destruction (Stallings & Brown, 2018; Whitman & Mattord, 2021). In tertiary education, cybersecurity extends beyond protecting computers and networks. It encompasses the protection of student records, staff information, examination materials, financial transactions, research data, intellectual property, and institutional digital services.

The increasing digitisation of Nigerian tertiary institutions means that a successful cyberattack could have consequences extending beyond temporary technical inconvenience. A compromised student information system could expose personal information, while manipulation of examination databases could undermine the credibility and integrity of academic results. Similarly, ransomware or other forms of malware could disrupt teaching, registration, examination processing, research, and administrative activities (National Institute of Standards and Technology [NIST], 2024).

Higher education institutions present distinctive cybersecurity challenges because of their large and diverse user populations. Students, lecturers, administrative personnel, researchers, contractors, visitors, and external collaborators may all require access to institutional digital resources (Ayodele et al.2023). The openness required for academic collaboration can therefore create security challenges when access controls and cybersecurity practices are inadequate (Zawacki-Richter et al., 2019).

Human behaviour is particularly important in cybersecurity. Phishing, social engineering, weak passwords, password reuse, unsafe downloads, and inappropriate information sharing can expose organisations to cyberattacks even when technical security controls are available. Hadlington (2017) demonstrates the importance of human factors in understanding risky cybersecurity behaviour, while Parsons et al. (2015) emphasise the role of individual characteristics and security behaviour in organisational cybersecurity.

The Nigerian cybersecurity environment has also evolved through important legislative and regulatory developments. The *Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act, 2024* provides a legal framework for addressing cybercrime and related offences in Nigeria (Federal Republic of Nigeria, 2024). Similarly, the *Nigeria Data Protection Act, 2023* establishes a comprehensive legal framework for the protection of personal data and imposes obligations on organisations that process personal information (Federal Republic of Nigeria, 2023).

The protection of personal information is particularly important in tertiary institutions because they routinely process substantial quantities of student and staff data. Such information may include names, contact details, identification information, academic records, financial information, health-related records, and employment information. Consequently, cybersecurity and data protection should be treated as complementary components of institutional information governance rather than as completely separate responsibilities (Federal Republic of Nigeria, 2023).

Cyber resilience extends cybersecurity beyond prevention and protection to include an organisation's ability to prepare for, withstand, respond to, recover from, and adapt following cyber incidents. The NIST Cybersecurity Framework 2.0 provides a useful structure through its six functions: Govern, Identify, Protect, Detect, Respond, and Recover (NIST, 2024). Applying such a framework within tertiary institutions can help ensure that cybersecurity is integrated into institutional governance and risk management.

Digital trust is another important consideration. Students and staff must have confidence that institutional digital systems are secure, reliable, available, and capable of protecting their personal information. Weak cybersecurity can therefore damage not only systems and data but also institutional reputation and stakeholder confidence (World Economic Forum, 2024).

The central argument of this paper is that cybersecurity should not be treated solely as an Information Technology responsibility. Rather, it should be regarded as an institution-wide governance, risk-management, data-protection, and educational responsibility. Nigerian tertiary institutions need a comprehensive cybersecurity strategy that integrates people, processes, technology, data protection, incident response, and continuous improvement.

2. LITERATURE REVIEW

2.1 Concept of Cybersecurity

Cybersecurity encompasses the protection of information systems, networks, devices, applications, and data from cyber threats. Traditional information security is commonly organised around the confidentiality, integrity, and availability (CIA) triad (Stallings & Brown, 2018; Whitman & Mattord, 2021).

Confidentiality ensures that information is accessible only to authorised individuals. Integrity ensures that information remains accurate and protected from unauthorised modification, while availability ensures that authorised users can access systems and information when required.

These three principles are particularly important in tertiary education. Confidentiality is essential for protecting student and staff records; integrity is necessary for maintaining trustworthy examination and academic records; and availability is critical for learning management systems, registration platforms, payment systems, and other digital services.

Modern cybersecurity, however, extends beyond the CIA triad to incorporate authentication, accountability, privacy, risk management, resilience, and governance (NIST, 2024).

2.2 Cybersecurity in Higher Education

Higher education institutions have complex cybersecurity environments because they combine academic openness with large-scale information processing. Researchers may require access to specialised systems, students may use personal devices, and different academic and administrative units may operate different applications.

This complexity can produce fragmented security environments. Zawacki-Richter et al. (2019) emphasise that technological developments are increasingly embedded in higher education, creating a need for institutions to develop appropriate structures and competencies for managing emerging technologies.

Consequently, cybersecurity should be incorporated into institutional digital transformation strategies rather than being considered only after new systems have been deployed.

2.3 Cyber Threats Facing Tertiary Institutions

Phishing remains one of the most important threats because it exploits human trust and attempts to obtain credentials or sensitive information through deceptive communications. Social engineering similarly manipulates individuals into disclosing information or performing actions that compromise security (Hadlington, 2017).

Ransomware presents another significant threat because it can prevent access to critical institutional information and services. The NIST Cybersecurity Framework emphasises the importance of protective measures, detection, response, and recovery in reducing the impact of such incidents (NIST, 2024).

Credential theft is also a major concern. Weak or reused passwords can provide attackers with access to email accounts, student portals, cloud applications, and administrative systems. Multifactor authentication provides an additional layer of protection by requiring users to provide more than one authentication factor.

2.4 Cyber Resilience

Cyber resilience recognises that cybersecurity cannot guarantee the complete elimination of cyber incidents. Instead, organisations need the capability to anticipate threats, withstand attacks, maintain essential operations, respond effectively, and recover quickly (NIST, 2024).

The NIST Cybersecurity Framework 2.0 organises cybersecurity activities around six functions: Govern, Identify, Protect, Detect, Respond, and Recover (NIST, 2024). These functions provide a useful foundation for tertiary institutions seeking to develop comprehensive cyber-resilience programmes.

2.5 Data Protection and Privacy

Cybersecurity and data protection are closely related but distinct. Cybersecurity focuses largely on protecting systems, networks, and information against threats, while data protection addresses how personal information is collected, processed, stored, shared, retained, and destroyed.

The Nigeria Data Protection Act 2023 establishes principles and obligations for the lawful and secure processing of personal data in Nigeria (Federal Republic of Nigeria, 2023). Tertiary institutions should therefore implement technical and organisational safeguards appropriate to the sensitivity and volume of personal data they process.

These safeguards may include access control, encryption, data classification, secure storage, retention policies, privacy notices, breach-management procedures, and staff training (Federal Republic of Nigeria, 2023).

2.6 Human Factors in Cybersecurity

Technology alone cannot guarantee cybersecurity. Users remain an important component of an organisation's security environment. Research has demonstrated relationships between human behaviour, attitudes, personality characteristics, and cybersecurity practices (Hadlington, 2017; Parsons et al., 2015).

In tertiary institutions, students and staff make daily decisions involving passwords, links, attachments, devices, data sharing, and system access. Cybersecurity awareness programmes can therefore help users recognise phishing attempts, protect credentials, report suspicious activities, and handle sensitive information appropriately.

Cybersecurity awareness should be continuous rather than limited to annual orientation programmes.

2.7 Cybersecurity Education and Workforce Development

Tertiary institutions have a dual responsibility: they must protect their own information systems and produce graduates with the knowledge and skills required to protect the wider digital ecosystem.

Cybersecurity education should therefore combine theoretical knowledge with practical competencies in areas such as network security, ethical hacking, digital forensics, secure software development, cloud security, incident response, risk management, data protection, and cyber law.

The development of an appropriately skilled cybersecurity workforce is increasingly important as organisations face rapidly changing cyber threats (Furnell & Rajendran, 2018).

3. METHODOLOGY

This paper adopted an integrative literature review methodology. An integrative review allows findings from scholarly research, professional standards, legislation, and policy documents to be synthesised to develop a broader conceptual understanding of a research problem.

The literature was selected from peer-reviewed publications, recognised cybersecurity frameworks, Nigerian legislation, regulatory documents, and authoritative international reports. Particular attention was given to sources addressing cybersecurity, higher education, cyber resilience, data protection, human factors, and digital trust.

The analysis employed thematic synthesis. The reviewed literature was organised around six themes:

1. cybersecurity governance;
2. people and cybersecurity awareness;
3. technology and infrastructure;
4. data protection and privacy;
5. incident response and recovery; and
6. digital trust and continuous improvement.

The themes were subsequently integrated into the proposed Cyber-Resilient Tertiary Institution Framework (CR-TIF).

Because the study is conceptual and does not involve primary data collection, no statistical results are presented. The findings reported in the following section represent a synthesis of the literature and relevant policy frameworks.

4. RESULTS AND DISCUSSION

4.1 Cybersecurity as an Institutional Governance Responsibility

The literature indicates that cybersecurity should be treated as an institutional governance responsibility rather than an ICT function alone (NIST, 2024; World Economic Forum, 2024).

Senior management should provide strategic direction and adequate resources, while ICT personnel should implement and maintain technical controls. Academic and administrative departments should also understand their responsibilities for protecting information.

An effective institutional cybersecurity governance structure should therefore include cybersecurity policies, risk assessment, defined responsibilities, compliance monitoring, incident reporting, periodic auditing, and management oversight.

4.2 Human Behaviour as a Cybersecurity Risk

The reviewed literature demonstrates the importance of human behaviour in cybersecurity (Hadlington, 2017; Parsons et al., 2015). A technically sophisticated security environment can still be compromised if users disclose passwords, click malicious links, install unsafe software, or share sensitive information improperly.

Tertiary institutions should therefore establish continuous awareness programmes covering:

i. phishing and social engineering;

ii. password security;

iii. multifactor authentication;

iv. device protection;

v. privacy;

vi. safe use of institutional systems; and

vii. incident reporting.

Security awareness should be treated as an institutional culture rather than a one-time training activity.

4.3 Strengthening Technical Controls

The literature and cybersecurity frameworks support a defence-in-depth approach in which multiple security controls operate together (NIST, 2024; Stallings & Brown, 2018).

Tertiary institutions should consider implementing:

i. multifactor authentication;

ii. endpoint protection;

iii. firewalls;

iv. network segmentation;

v. encryption;

vi. vulnerability scanning;

vii. patch management;

viii. intrusion detection;

ix. identity and access management;

x. secure backups; and

xi. security monitoring.

Network segmentation is particularly important because it can limit the movement of attackers following the compromise of one system.

4.4 Data Protection and Privacy

The Nigeria Data Protection Act 2023 reinforces the need for institutions to protect personal information through appropriate technical and organisational measures (Federal Republic of Nigeria, 2023).

Institutions should identify the categories of information they hold, determine who requires access, establish appropriate retention periods, and ensure secure disposal when information is no longer required.

A practical data classification model could distinguish between public, internal, confidential, sensitive, and highly sensitive information. Examination materials, authentication credentials, sensitive student information, and critical research data should receive enhanced protection.

4.5 Incident Response and Recovery

The NIST Cybersecurity Framework emphasises detection, response, and recovery as essential components of cybersecurity resilience (NIST, 2024).

Tertiary institutions should therefore maintain formal incident-response plans specifying:

i. who receives incident reports;
ii. who has authority to isolate systems;
iii. how evidence is preserved;
iv. how affected users are informed;
v. how critical services are restored;
vi. how regulatory obligations are addressed; and
vii. how lessons learned are incorporated into future controls.

Institutions should also conduct periodic tabletop exercises and test backup restoration procedures.

4.6 Digital Trust as an Institutional Asset

Digital trust is closely connected to cybersecurity, privacy, reliability, and institutional accountability. When students and staff believe that institutional systems are secure and reliable, they are more likely to adopt digital services.

Conversely, significant breaches can damage institutional reputation and stakeholder confidence (World Economic Forum, 2024).

Consequently, cybersecurity investment should be viewed not merely as a technical expense but as an investment in institutional credibility, service continuity, and stakeholder trust.

4.7 Proposed Cyber-Resilient Tertiary Institution Framework

Based on the literature, this paper proposes the **Cyber-Resilient Tertiary Institution Framework (CR-TIF)** comprising six interconnected pillars:

Pillar 1: Governance and Policy
Cybersecurity strategy, institutional policies, risk management, compliance, accountability, and leadership.

Pillar 2: People and Awareness
Student and staff awareness, cybersecurity culture, training, phishing simulations, and incident reporting.

Pillar 3: Technology and Infrastructure
Multifactor authentication, encryption, network segmentation, endpoint security, patch management, backups, and monitoring.

Pillar 4: Data Protection and Privacy
Data classification, access control, privacy-by-design, secure retention, secure disposal, and compliance with the Nigeria Data Protection Act 2023.

Pillar 5: Incident Response and Recovery
Detection, containment, communication, evidence preservation, disaster recovery, business continuity, and post-incident review.

Pillar 6: Continuous Improvement and Digital Trust
Security audits, maturity assessments, policy reviews, emerging-threat monitoring, stakeholder communication, and continuous improvement.

The proposed framework:

Cyber Threats → Risk Identification → Governance + People + echnology + Data Protection → Detection → Response → Recovery → Continuous Improvement → Digital Trust

This relationship is consistent with the risk-management and cybersecurity lifecycle principles reflected in NIST (2024) and ISO/IEC 27001 (International Organization for Standardization, 2022).

4.8 Implications for Nigerian Tertiary Institutions

The findings suggest that Nigerian tertiary institutions should integrate cybersecurity into their wider digital transformation strategies.

Security requirements should be considered when systems are designed and procured rather than after implementation.

Institutions should also strengthen collaboration between ICT units, academic departments, management, data protection personnel, legal/compliance units, and cybersecurity professionals.

Furthermore, cybersecurity education should become increasingly practical. Students should be exposed to laboratories, simulations, ethical hacking exercises, digital forensics, secure coding, incident-response exercises, and industry-based projects.

5. CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

The digital transformation of Nigerian tertiary institutions offers substantial benefits but simultaneously creates increased cybersecurity risks. The growing dependence on online learning platforms, student information systems, electronic payment systems, cloud services, research platforms, and digital communication increases the importance of cybersecurity.

The literature reviewed demonstrates that effective cybersecurity requires more than technical controls. Human behaviour, governance, data protection, incident response, institutional policy, and continuous improvement are equally important (NIST, 2024; World Economic Forum, 2024).

The Nigeria Data Protection Act 2023 and the Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act 2024 provide important legal foundations for protecting data and addressing cybercrime in Nigeria (Federal Republic of Nigeria, 2023, 2024).

The proposed Cyber-Resilient Tertiary Institution Framework integrates governance, people, technology, data protection, incident response, and continuous improvement. Its central premise is that cybersecurity should become an institution-wide responsibility.

For Nigerian tertiary institutions, cyber resilience should therefore be viewed as a strategic requirement for sustainable digital transformation. Institutions that successfully protect their systems and data will be better positioned to maintain educational continuity, protect stakeholder privacy, preserve institutional reputation, and strengthen digital trust.

5.2 Recommendations

1. **Develop comprehensive institutional cybersecurity policies.**
   Nigerian tertiary institutions should develop and periodically update institution-wide cybersecurity policies aligned with relevant legislation and recognised frameworks (Federal Republic of Nigeria, 2023, 2024; NIST, 2024).

2. **Establish cybersecurity governance structures.**
   Management should establish appropriate cybersecurity governance mechanisms with clear responsibilities and accountability.

3. **Conduct regular cybersecurity risk assessments.**
   Institutions should regularly identify critical assets, vulnerabilities, threats, and potential impacts.

4. **Implement multifactor authentication.**
   MFA should be prioritised for email, administrative systems, financial platforms, learning management systems, and other sensitive services.

5. **Strengthen cybersecurity awareness programmes.**
   Staff and students should receive regular training in phishing, social engineering, password security, privacy, and incident reporting (Hadlington, 2017).

6. **Implement data classification and protection.**
   Institutional information should be classified according to sensitivity and protected using controls appropriate to its risk level.

7. **Develop incident-response and recovery plans.**
   Institutions should establish, test, and continuously improve incident-response and disaster-recovery procedures (NIST, 2024).

8. **Strengthen cybersecurity laboratories.**
   Computer Science and related programmes should provide practical cybersecurity laboratories where students can develop industry-relevant competencies.

9. **Promote industry and professional collaboration.**
   Institutions should partner with cybersecurity organisations, professional bodies, government agencies, and industry to strengthen training and knowledge exchange.

10. **Integrate cybersecurity into digital transformation projects.**
    Security and privacy requirements should be incorporated at the planning and design stages of digital projects.

11. **Conduct periodic security audits.**
    Independent assessments should be used to identify weaknesses and evaluate institutional cybersecurity maturity.

12. **Promote cybersecurity research.**
    Nigerian tertiary institutions should encourage research into emerging areas such as AI-enabled cyberattacks, ransomware, cloud security, privacy-preserving technologies, IoT security, cybercrime, and cyber resilience.

13. **Build a culture of digital trust.**
    Institutions should communicate clearly about how personal information is protected, how incidents are handled, and what users can do to protect themselves.

Ultimately, cybersecurity should be regarded as a foundation of digital transformation, educational continuity, data protection, institutional reputation, and digital trust in Nigerian tertiary education.

References

Ayodele, O. S., Aliu, J., Owoeye, F. O., Ajayi, E. A., & Sheidu, A. Y. (2023). The role of artificial intelligence in curriculum development and management. Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology, 11(1), 37–46. https://doi.org/10.22624/AIMS/DIGITAL/V11N2P4.

Federal Republic of Nigeria. (2023). *Nigeria Data Protection Act, 2023*.

Federal Republic of Nigeria. (2024). *Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act, 2024*.

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 information security, cybersecurity and privacy protection—Information security management systems—Requirements*.

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

Parsons, K., Butavicius, M., Delfabbro, P., & Lillie, M. (2015). Predicting security behaviour: Examining the predictive power of a personality trait model. *Proceedings of the 23rd Australian Computer-Human Interaction Conference*, 241–249. https://doi.org/10.1145/2828959.2828976

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Pearson.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage.

World Economic Forum. (2024). *Global cybersecurity outlook 2024*. World Economic Forum.

Zawacki-Richter, O., Marín, V. I., Bond, M., & Gouverneur, F. (2019). Systematic review of research on artificial intelligence applications in higher education—Where are the educators? *International Journal of Educational Technology in Higher Education, 16*, Article 39. https://doi.org/10.1186/s41239-019-0171-0
:::

Artificial Intelligence-Driven Analysis of Chemical Contaminants and Radiation Exposure Risks in Environmental and Biological Samples

Omananyi Muhammed Rabiu, Salihu Abubakar

Department of Science Laboratory Technology, Kogi State Polytechnic, Lokoja

Abstract

The increasing occurrence of chemical contaminants and ionizing radiation in environmental and biological systems presents complex challenges for public health, environmental protection, and radiation safety. Conventional analytical approaches such as gas chromatography–mass spectrometry, liquid chromatography–mass spectrometry, inductively coupled plasma–mass spectrometry, and gamma-ray spectrometry provide reliable measurements but generate large, multidimensional datasets that may be difficult to interpret rapidly and integrate across exposure pathways. Artificial intelligence (AI), particularly machine learning (ML) and deep learning, offers opportunities to improve contaminant identification, concentration prediction, exposure assessment, pattern recognition, and health-risk characterization. This article examines an integrated AI-driven framework for analysing chemical contaminants and radiation exposure risks in environmental and biological samples. The study adopts a structured literature-review and conceptual modelling approach, drawing on evidence from analytical chemistry, environmental health, radiation protection, dosimetry, and AI research. Environmental and biological matrices considered include soil, water, food, air particulates, blood, urine, and other biological specimens. The proposed framework integrates analytical chemistry measurements, radionuclide activity concentrations, radiation dose parameters, physicochemical characteristics, exposure pathways, and biological indicators into machine-learning models. The literature indicates that AI can support chemical classification, contaminant prediction, anomaly detection, mixture-risk assessment, spatial exposure mapping, and radiation-dose prediction. However, model reliability depends strongly on data quality, analytical uncertainty, sample representativeness, explainability, validation, and appropriate radiation-protection assumptions. The article concludes that combining analytical chemistry with radiation health physics and AI can provide a more holistic approach to environmental and biological risk assessment. It recommends development of validated multidisciplinary datasets, explainable AI models, standardized analytical protocols, uncertainty-aware modelling, and collaboration among analytical chemists, radiation health physicists, environmental scientists, data scientists, and public-health professionals.

Keywords: artificial intelligence, analytical chemistry, chemical contaminants, radiation health physics, machine learning, environmental samples, biological samples, risk assessment, dosimetry

1. Introduction

Environmental contamination has become an increasingly important public-health and environmental-management concern because populations may be exposed simultaneously to chemical, biological, and physical hazards. Chemical contaminants may originate from industrial activities, agricultural practices, mining, petroleum operations, waste disposal, domestic activities, and naturally occurring geological processes. Examples include heavy metals, pesticides, polycyclic aromatic hydrocarbons (PAHs), volatile and semivolatile organic compounds, persistent organic pollutants, pharmaceuticals, and emerging contaminants. At the same time, environmental and occupational exposure to ionizing radiation may arise from naturally occurring radioactive materials, radon, mining activities, medical applications, industrial sources, radioactive waste, and accidental releases (Wang et al., 2024).

Ionizing radiation occurs naturally in soil, water, air, food, and living organisms, while artificial sources are widely used in medicine, industry and research. The World Health Organization (WHO, 2023a) notes that radiation exposure may occur through external irradiation or internal contamination following inhalation, ingestion, or other routes. The health implications of exposure depend on factors including radiation type, absorbed dose, dose rate, exposure duration and the sensitivity of the exposed tissue.

The assessment of environmental contaminants traditionally depends on laboratory-based analytical chemistry. Techniques such as gas chromatography–mass spectrometry (GC-MS), liquid chromatography–mass spectrometry (LC-MS), atomic absorption spectrometry (AAS), inductively coupled plasma–mass spectrometry (ICP-MS), and related chromatographic and spectrometric techniques enable the detection and quantification of chemical contaminants. For example, the U.S. Environmental Protection Agency (EPA) Method 6020B provides an ICP-MS approach for determining selected elements in environmental matrices, while Method 8270E provides a GC-MS approach for semivolatile organic compounds (Kadadou et al., 2024).

Radiation health physics, on the other hand, focuses on the measurement, assessment and control of exposure to ionizing radiation. Radiation measurements may involve gross alpha/beta counting, gamma-ray spectrometry, alpha spectrometry, radon measurements, thermoluminescent dosimetry, optically stimulated luminescence, personal dosimetry and other techniques. The International Commission on Radiological Protection (ICRP) system provides a framework for relating measurements and exposure pathways to radiation-protection quantities. UNSCEAR's recent assessment of public exposure emphasizes the importance of evaluating both natural and human-made sources and of understanding spatial, temporal and environmental variations in radiation exposure (United Nations Scientific Committee on the Effects of Atomic Radiation [UNSCEAR], 2024).

The increasing complexity of environmental and biological datasets creates an opportunity for artificial intelligence. AI encompasses computational approaches capable of learning patterns from data and supporting prediction, classification, anomaly detection and decision-making. Machine learning algorithms such as random forests, support vector machines, artificial neural networks, gradient boosting and deep learning models have increasingly been applied to analytical chemistry and environmental-health problems.

Recent literature indicates that AI has become increasingly relevant to analytical chemistry through applications in data processing, chemometric modelling, experimental design and interpretation of complex analytical datasets (Nowak, 2026). Similarly, AI is increasingly being considered for environmental-health research involving data integration, hazard identification, risk assessment and management of complex or combined exposures (Huang et al., 2025).

The challenge, however, is that chemical and radiation exposures are often assessed separately. Such separation may not adequately represent real-world exposure conditions in which individuals may encounter multiple chemical contaminants and radiation sources simultaneously. Moreover, interactions among environmental variables, contaminant concentrations, exposure pathways and biological responses can create nonlinear relationships that conventional statistical methods may not easily capture.

This article therefore proposes an integrated AI-driven approach that combines analytical chemistry measurements with radiation health-physics parameters for environmental and biological risk assessment. The objectives are to:

1. examine the role of analytical chemistry in generating data for AI-based contaminant assessment;
2. examine the application of AI and machine learning to chemical contaminant analysis;
3. examine AI applications in radiation exposure and dosimetry assessment;
4. propose an integrated framework for combining chemical and radiation exposure data; and
5. identify the opportunities, limitations and requirements for implementing AI-driven environmental and biological risk assessment.

2. Literature Review

2.1 Chemical Contaminants in Environmental and Biological Samples

Environmental contaminants occur in a wide range of matrices. Water, soil, sediments, food, air and biological tissues can contain mixtures of organic and inorganic pollutants. Biological samples such as blood, urine, hair, breast milk and tissues can also provide evidence of internal exposure.

Heavy metals and metalloids such as lead, cadmium, mercury, arsenic and chromium are of particular concern because some may persist in the environment and accumulate in biological systems. Analytical chemistry provides the foundation for detecting and quantifying such contaminants. ICP-MS is particularly valuable because of its sensitivity and ability to determine multiple elements in a single analytical run. EPA Method 6020B, for example, identifies ICP-MS as an analytical method for determining selected elemental contaminants in environmental samples (Tchounwou et al., 2014).

Organic contaminants present another analytical challenge because environmental samples may contain numerous compounds at different concentrations. GC-MS is widely applied to semivolatile organic compounds, while LC-MS and high-resolution mass spectrometry are useful for compounds that are thermally unstable, polar or unsuitable for gas chromatography. EPA Method 8270E illustrates the application of GC-MS to semivolatile organic compounds in environmental matrices (Gonçalo Catarro et al., 2025).

The complexity of modern analytical instruments has produced increasingly large datasets. Chromatograms, mass spectra and spectral fingerprints can contain thousands of variables. Traditional interpretation may require substantial expert knowledge and may be affected by overlapping peaks, background interference, matrix effects and low analyte concentrations.

2.2 Artificial Intelligence in Analytical Chemistry

AI provides several opportunities for processing complex analytical datasets. Machine-learning algorithms can learn relationships between analytical signals and known chemical classes or concentrations. Supervised learning can be used when labelled datasets are available, whereas unsupervised learning can identify hidden patterns without predefined classes (Ayodele et al., 2023).

Applications include:

i. chemical classification;
ii. spectral interpretation;
iii. peak identification;
iv. quantitative prediction;
v. anomaly detection;
vi. contaminant source identification;
vii. multicomponent analysis;
viii. process optimization; and
ix. prediction of chemical toxicity.

AI is increasingly recognized as a significant development in analytical chemistry. Nowak (2026) notes that AI has already become embedded in areas such as data processing and chemometric modelling while highlighting the need for appropriate evaluation and uncertainty analysis of AI-based analytical systems.

Machine learning is also increasingly used for environmental chemical-risk assessment. Recent work emphasizes its potential to address complex mixtures, where conventional assessments based on individual chemicals may not adequately reflect real-world exposure (Huang et al., 2025).

2.3 Radiation Exposure and Health Physics

Radiation health physics involves protecting people and the environment from unnecessary exposure to ionizing radiation. Radiation may be received through external irradiation or internal exposure following the intake of radioactive materials.

The absorbed dose is expressed in gray (Gy), while equivalent and effective doses are expressed in sievert (Sv). Radiation risk is influenced by the amount and type of radiation, exposure duration, dose rate, route of exposure and characteristics of the exposed population (WHO, 2023a).

Environmental radiation may originate from naturally occurring radionuclides such as uranium, thorium, radium and potassium-40, as well as radon and its decay products. Human-made sources may include medical, industrial and research applications. UNSCEAR (2024) reports that natural sources remain the major contributors to global public exposure, although human-made exposures can become important under particular circumstances.

Radon represents an important example of environmental radiation exposure. It is a naturally occurring radioactive gas generated during the decay of uranium in rocks and soil and can accumulate in enclosed environments (WHO, 2023b).

2.4 Artificial Intelligence in Radiation Health Physics

AI has increasingly been applied in medical physics, radiation oncology, imaging and radiation-dose prediction. Deep-learning approaches, for example, have been investigated for predicting radiotherapy dose distributions and improving treatment planning (Kazemzadeh et al., 2025).

The same principles can potentially be extended to environmental radiation assessment. AI can analyse relationships between radiation measurements and variables such as geological characteristics, soil composition, land use, distance from radiation sources, meteorological parameters, population characteristics and exposure pathways.

Potential applications include:

1. prediction of environmental radiation levels;
2. identification of radiation hotspots;
3. classification of areas according to exposure risk;
4. prediction of internal and external dose;
5. anomaly detection in radiation-monitoring systems;
6. spatial and temporal mapping of radiation;
7. identification of factors contributing to radiation exposure; and
8. early warning during unusual radiation events.

UNSCEAR (2024) emphasizes the importance of evaluating geographical and environmental features, temporal trends and uncertainties in public exposure assessment. These requirements align well with the capacity of AI to process multidimensional datasets.

2.5 Combined Chemical and Radiation Exposure

One of the major gaps in environmental health research is the separation of chemical and physical hazards during risk assessment. In real environments, individuals may encounter multiple contaminants simultaneously. These may include heavy metals, organic pollutants, radionuclides and other environmental stressors.

Combined exposure is particularly important because biological responses may involve oxidative stress, inflammation, DNA damage and other mechanisms. However, the magnitude and nature of interactions cannot be assumed to be additive without appropriate experimental evidence.

AI offers an opportunity to model complex exposure scenarios. Huang et al. (2025) identified AI-driven data integration and modelling as important opportunities for understanding complex environmental-health exposures.

Similarly, recent literature on AI and chemical-mixture toxicity demonstrates the growing application of machine learning to chemical mixtures rather than isolated substances (Application of machine learning and artificial intelligence methods in toxicity and risk assessment of chemical mixtures, 2026).

3. Methodology

3.1 Research Design

This article adopted a structured integrative literature-review and conceptual modelling design. The approach was selected because the objective was to synthesize knowledge from analytical chemistry, environmental toxicology, radiation health physics and artificial intelligence and develop an integrated framework.

The study did not claim to generate new laboratory measurements. Consequently, numerical findings presented in Section 4 represent literature-derived findings and proposed analytical outcomes, rather than experimentally generated results.

3.2 Data Sources

Relevant literature and authoritative technical information were obtained from peer-reviewed scientific publications and institutional sources including:

- WHO;
- UNSCEAR;
- U.S. EPA;
- radiation-protection literature;
- analytical chemistry literature;
- environmental-health literature; and
- artificial-intelligence and machine-learning research.

The literature was examined for evidence concerning:

1. chemical contaminant measurement;
2. radiation measurement and dosimetry;
3. AI applications in analytical chemistry;
4. AI applications in environmental health;
5. AI applications in radiation assessment;
6. chemical-mixture assessment;
7. exposure prediction; and
8. health-risk modelling.

3.3 Proposed Integrated Dataset

The proposed AI system would integrate four major categories of variables:

A. Analytical chemistry variables

These may include:

- concentrations of heavy metals;
- pesticide concentrations;
- PAH concentrations;
- organic contaminant profiles;
- elemental concentrations;
- chromatographic peak characteristics;
- mass spectral features; and
- physicochemical parameters.

B. Radiation variables

These may include:

- radionuclide activity concentration (Bq/kg or Bq/L);
- ambient dose rate (µSv/h);
- absorbed dose;
- annual effective dose;
- radon concentration;
- exposure duration;
- internal dose estimates; and
- external dose estimates.

C. Environmental variables

Potential variables include:

- geographical coordinates;
- soil characteristics;
- pH;
- temperature;
- rainfall;
- land use;
- distance from industrial activities;
- geological characteristics; and
- water-quality parameters.

D. Biological variables

Where ethically and scientifically appropriate, biological indicators may include:

- contaminant concentrations in blood or urine;
- biomarkers of exposure;
- biomarkers of oxidative stress;
- biochemical indicators;
- demographic variables;
- exposure history; and
- relevant clinical or physiological indicators.

3.4 Analytical Techniques

The proposed analytical workflow may employ ICP-MS for elemental contaminants, GC-MS for selected semivolatile organic compounds, LC-MS for suitable polar and thermally labile compounds, and gamma spectrometry for radionuclide identification and quantification. EPA analytical methods provide examples of validated approaches for chemical determination in environmental matrices.

Radiation measurements may be obtained using calibrated gamma spectrometers, survey meters, dosimeters and radon-monitoring instruments, depending on the research question and radiation source.

3.5 Data Preprocessing

Before AI modelling, the following procedures are proposed:

1. removal of duplicate records;
2. identification and treatment of missing values;
3. detection of analytical outliers;
4. normalization or standardization;
5. correction for batch effects;
6. dimensionality reduction;
7. feature selection;
8. treatment of censored measurements;
9. integration of measurement uncertainties; and
10. separation of training, validation and testing datasets.

Particular attention should be given to analytical uncertainty because an AI model trained on inaccurate or poorly characterized laboratory data may produce apparently precise but scientifically unreliable predictions.

3.6 Machine-Learning Models

Several AI approaches may be evaluated.

Random Forest (RF): Useful for classification, regression and ranking predictor importance.

Support Vector Machine (SVM): Useful for classification of chemical or radiation exposure categories, particularly with moderately sized datasets.

Artificial Neural Networks (ANN): Suitable for modelling nonlinear relationships between multiple exposure variables and outcomes.

Gradient Boosting Models: Useful for prediction where complex nonlinear interactions exist.

Deep Learning: Appropriate for large datasets such as mass spectra, chromatographic signals, hyperspectral images or high-frequency radiation-monitoring data.

Unsupervised learning: Clustering techniques may be used to identify exposure profiles or geographic zones with similar chemical-radiation characteristics.

3.7 Model Evaluation

The models should be evaluated using appropriate metrics. For classification, accuracy, precision, recall, F1-score and area under the receiver operating characteristic curve may be used. For regression, root mean square error (RMSE), mean absolute error (MAE) and coefficient of determination (R^2) may be employed.

Cross-validation should be applied to reduce overfitting. An independent test dataset should be retained to evaluate generalization.

3.8 Explainability and Uncertainty

AI outputs should not be treated as automatically correct. Explainable AI approaches, including feature-importance analysis and SHAP-based interpretation, can help identify variables contributing most strongly to predictions.

Uncertainty should be reported alongside model predictions. This is particularly important for radiation-risk assessment because uncertainties can arise from measurement errors, sampling variability, dosimetric assumptions, exposure duration and individual differences. UNSCEAR has specifically emphasized the importance of uncertainty in radiation-risk assessment (UNSCEAR, 2012).

4. Results and Discussion

4.1 Literature-Derived Findings

The reviewed evidence demonstrates that AI has substantial potential for integrating chemical and radiation data. Four major findings emerged.

4.1.1 AI improves interpretation of complex analytical datasets

Modern analytical instruments generate multidimensional datasets that can contain large numbers of chemical features. AI can reduce the burden of manual interpretation by identifying patterns, classifying samples and predicting contaminant concentrations.

This is particularly important where environmental samples contain multiple contaminants. Conventional approaches may examine each contaminant independently, whereas machine-learning models can consider several variables simultaneously. Recent environmental-health research identifies data integration and AI-based modelling as promising approaches for complex and combined exposure assessment (Huang et al., 2025).

4.1.2 AI can support radiation-exposure prediction

The literature on AI applications in radiation medicine demonstrates that machine learning and deep learning can model complex relationships involving radiation dose and anatomical or treatment parameters (Kazemzadeh et al., 2025).

In environmental radiation health physics, similar approaches can be adapted to predict radiation exposure from environmental variables. A model could, for example, estimate exposure risk using radionuclide concentrations, ambient dose rates, soil characteristics, geographic location and human activity patterns.

However, environmental radiation predictions must remain consistent with established dosimetric principles. AI should therefore complement, rather than replace, radiation measurements and established dose-assessment methods.

4.1.3 Integrated modelling can identify high-risk exposure profiles

A major advantage of the proposed framework is the ability to combine chemical and radiation variables.

For example, a hypothetical environmental-health dataset could contain:

$$X = C_1, C_2, \dots, C_n, R_1, R_2, \dots, R_m, E_1, E_2, \dots, E_k$$

where (C) represents chemical-contaminant measurements, (R) represents radiation variables, and (E) represents environmental and exposure variables.

The AI model can then estimate an outcome:

$$Y = f(C, R, E)$$

where (Y) may represent an exposure-risk category, predicted effective dose, contaminant burden or another scientifically defined endpoint.

This framework is particularly valuable for identifying exposure profiles that may not be apparent when chemical and radiation datasets are analysed independently.

4.1.4 AI is particularly useful for anomaly detection

Radiation-monitoring systems can generate continuous measurements. AI algorithms can identify unusual deviations from expected background patterns and potentially support early investigation.

Similarly, AI can identify unusual chemical fingerprints in analytical datasets. Anomalies may indicate contamination events, industrial releases, laboratory errors or unusual environmental conditions.

This application is consistent with the broader movement toward AI-supported environmental-health monitoring and risk management (Huang et al., 2025).

4.2 Proposed Integrated AI Framework

The proposed framework consists of six interconnected stages:

Environmental and biological sampling → Laboratory analysis → Data integration → AI modelling → Exposure/risk prediction → Decision support

Stage 1: Sampling

Environmental samples such as water, soil, sediment, food and air particulates are collected using scientifically appropriate sampling designs. Biological samples may be collected where ethically approved.

Stage 2: Laboratory analysis

Chemical contaminants are measured using validated analytical techniques. Radiation measurements are conducted using calibrated radiation-detection and dosimetry systems.

Stage 3: Data integration

Chemical, radiation, environmental and biological data are combined in a structured database. Metadata concerning sample location, date, analytical method and measurement uncertainty should also be retained.

Stage 4: AI modelling

Machine-learning algorithms identify relationships between the input variables and defined outcomes.

Stage 5: Risk prediction

The model generates predicted exposure levels or risk categories. Where appropriate, results may be converted into established exposure or dose metrics.

Stage 6: Decision support

The final outputs can support environmental monitoring, occupational protection, public-health surveillance, remediation and regulatory decision-making.

4.3 Implications for Environmental Health

The integration of AI with analytical chemistry and radiation health physics could shift environmental health assessment from isolated measurements toward multidimensional exposure profiling.

Traditional monitoring may answer questions such as:

What concentration of lead is present?

or:

What is the ambient radiation dose rate?

An integrated AI approach can address more complex questions:

What combination of chemical contaminants, radionuclides, environmental characteristics and exposure pathways contributes most strongly to the predicted risk in a particular population or location?

This shift is particularly relevant because humans are rarely exposed to only one environmental stressor. Recent work on AI and environmental health emphasizes the need for data fusion and modelling of complex exposures (Huang et al., 2025).

4.4 Challenges and Limitations

Despite its potential, AI-based environmental and radiation-health assessment has important limitations.

Data quality

AI cannot compensate for poor analytical data. Incorrect sampling, contamination, calibration errors and inadequate detection limits can introduce systematic errors into the model.

Dataset size

Deep-learning models generally require substantial datasets. In many environmental and radiation-health applications, datasets may be relatively small or geographically restricted.

Model interpretability

A highly accurate black-box model may be difficult for scientists, regulators and health professionals to trust. Explainability is therefore essential.

Generalizability

A model developed using data from one geographical region may perform poorly in another because of differences in geology, climate, industrial activities, contaminant profiles and population characteristics.

Measurement uncertainty

Both analytical chemistry and radiation measurements contain uncertainty. The AI framework should incorporate these uncertainties rather than treating every measurement as exact.

Ethical and privacy concerns

Biological and health-related datasets may contain sensitive information. Data governance, anonymization and appropriate ethical approval are therefore necessary.

Regulatory acceptance

AI predictions should not automatically replace validated laboratory methods or established radiation-protection calculations. The recent literature on AI and regulatory toxicology highlights concerns regarding transparency, reliability and regulatory acceptance (Bridging AI advancements with risk assessment needs, 2026).

5. Conclusions and Recommendations

5.1 Conclusion

The integration of artificial intelligence, analytical chemistry and radiation health physics provides a promising multidisciplinary framework for environmental and biological risk assessment. Analytical chemistry supplies quantitative information about chemical contaminants, while radiation health physics provides measurements and models for assessing exposure to ionizing radiation. Artificial intelligence provides computational tools capable of integrating these heterogeneous datasets and identifying nonlinear relationships, patterns, anomalies and potential risk profiles.

The literature reviewed indicates that AI can contribute to chemical contaminant classification, concentration prediction, mixture analysis, exposure assessment, radiation monitoring, dose prediction and environmental-health decision support. Its greatest potential lies in integrating information that is traditionally analysed separately.

However, AI should be regarded as a decision-support technology rather than a substitute for validated laboratory measurements, calibrated radiation instruments, established dosimetric models or expert judgement. The reliability of AI predictions depends fundamentally on the quality, representativeness and traceability of the underlying data.

An integrated approach is therefore particularly relevant for environmental settings where chemical and radiation hazards may coexist. Such a framework could support more timely identification of contaminated locations, improved exposure characterization and more efficient environmental-health surveillance.

5.2 Recommendations

Based on the findings of this review, the following recommendations are proposed:

1. **Development of multidisciplinary databases:** Researchers should establish standardized databases combining chemical contaminant concentrations, radionuclide measurements, radiation dose parameters, environmental characteristics and biological indicators.
2. **Integration of uncertainty:** AI models should incorporate analytical and dosimetric uncertainty rather than treating measurements as error-free.
3. **Use of explainable AI:** Explainable machine-learning approaches should be prioritized so that scientists and regulators can understand the factors influencing predictions.
4. **Standardization of analytical procedures:** Sample collection, preparation, chemical analysis, radiation measurement and quality-control procedures should follow validated protocols.
5. **Independent model validation:** AI models should be tested using independent datasets obtained from different locations and time periods.
6. **Interdisciplinary collaboration:** Analytical chemists, radiation health physicists, environmental scientists, computer scientists, epidemiologists and public-health professionals should collaborate in developing AI-based environmental-health systems.
7. **Ethical data governance:** Biological and health-related information should be anonymized and managed according to applicable ethical and data-protection requirements.
8. **AI-assisted environmental monitoring:** Government agencies, research institutions and industries should explore AI-enabled monitoring systems capable of detecting unusual chemical and radiation patterns.
9. **Capacity building:** Universities and research institutions should develop

interdisciplinary training in analytical chemistry, radiation health physics, data science and AI.

10. **Pilot studies in high-risk environments:** Future empirical studies should validate the proposed framework using real environmental and biological samples from selected Nigerian locations, particularly areas influenced by mining, industrial activities, waste disposal or other potential sources of chemical and radiological exposure.

References

Ayodele, O. S., Aliu, J., Owoeye, F. O., Ajayi, E. A., & Alabi, T. J. (2023). *Google scholar*. Google.Com. https://scholar.google.com/scholar?oi=bibs&cluster=10033191537579164140&btnI=1&hl=en

Bridging AI advancements with risk assessment needs: A journey towards effective use and regulatory acceptance. (2026). *Toxicology, 523*, 154439. https://doi.org/10.1016/j.tox.2026.154439

Gonçalo Catarro, Pelixo, R., Feijó, M., Rosado, T., Socorro, S., André R. T. S. Araújo, & Gallardo, E. (2025). Analytical approaches using GC-MS for the detection of pollutants in wastewater towards environmental and human health benefits: A comprehensive review. *Chemosensors*, *13*(7), 253–253. https://doi.org/10.3390/chemosensors13070253

Huang, L., Duan, Q., Liu, Y., Wu, Y., Li, Z., Guo, Z., Liu, M., Lu, X., Wang, P., Liu, F., Ren, F., Li, C., Wang, J., Huang, Y., Yan, B., Kioumourtzoglou, M.-A., & Kinney, P. L. (2025). Artificial intelligence: A key fulcrum for addressing complex environmental health issues. *Environment International, 198*, 109389. https://doi.org/10.1016/j.envint.2025.109389

Kadadou, D., Tizani, L., & Hasan, S. W. (2024). Analytical methods for determining environmental contaminants of concern in water and wastewater. *MethodsX*, *12*, 102582–102582. https://doi.org/10.1016/j.mex.2024.102582

Kazemzadeh, A., Rasti, R., & Tavakoli, M. B. (2025). Artificial intelligence for radiotherapy dose prediction: A comprehensive review. *Cancer/Radiothérapie*. https://doi.org/10.1016/j.canrad.2025.104630

Nowak, P. M. (2026). Artificial intelligence in analytical chemistry: Towards yet undiscovered opportunities. *Analytical Chemistry, 98*(8), 5843–5853. https://doi.org/10.1021/acs.analchem.5c06840

Tchounwou, P. B., Yedjou, C. G., Patlolla, A. K., & Sutton, D. J. (2014). Heavy metal toxicity and the environment. *Experientia Supplementum*, *101*(1), 133–164. https://doi.org/10.1007/978-3-7643-8340-4_6

U.S. Environmental Protection Agency. (2014a). *Method 6020B (SW-846): Inductively coupled plasma-mass spectrometry*. U.S. Environmental Protection Agency. (US EPA)

U.S. Environmental Protection Agency. (2014b). *Method 8270E (SW-846): Semivolatile organic compounds by gas chromatography/mass spectrometry (GC/MS)*. U.S. Environmental Protection Agency. (US EPA)

United Nations Scientific Committee on the Effects of Atomic Radiation. (2012). *Sources and effects of ionizing radiation: UNSCEAR 2012 report to the General Assembly, with scientific annexes*. United Nations.

United Nations Scientific Committee on the Effects of Atomic Radiation. (2024). *Sources, effects and risks of ionizing radiation: UNSCEAR 2024 report, Volume II, Scientific Annex B: Evaluation of public exposure to ionizing radiation*. United Nations. (UNSCEAR)

Wang, F., Xiang, L., Sze-Yin Leung, K., Elsner, M., Zhang, Y., Guo, Y., Pan, B., Sun, H., An, T., Ying, G., Brooks, B. W., Hou, D., Helbling, D. E., Sun, J., Qiu, H., Vogel, T. M., Zhang, W., Gao, Y., Simpson, M. J., … Tiedje, J. M. (2024). Emerging contaminants: A one health perspective. *The Innovation*, *5*(4), 100612. https://doi.org/10.1016/j.xinn.2024.100612

World Health Organization. (2023a, July 27). *Ionizing radiation and health effects*. https://www.who.int/news-room/fact-sheets/detail/ionizing-radiation-and-health-effects (World Health Organization)

World Health Organization. (2023b, July 7). *Radiation and health*. https://www.who.int/news-room/questions-and-answers/item/radiation-and-health (World Health Organization)

World Health Organization. (2023c). *Radon*. https://www.who.int/teams/environment-climate-change-and-health/radiation-and-health/environmental-exposure/radon (World Health Organization)

Molecular Characterization of *Salmonella* Isolates from Selected Poultry Farms in Zaria Metropolis, Kaduna State, Nigeria

Aminu Isa[1], Ibrahim Mohammed Hussaini[2] & Omananyi Muhammed Rabiu[1]

[1] Department of Science Laboratory Technology, Kogi State Polytechnic, Lokoja, Nigeria

[2] Department of Microbiology, Faculty of Life Sciences, Ahmadu Bello University, Zaria, Nigeria

Corresponding author: Aminu Isa
E-mail: aminuisaa@gmail.com

Abstract

Salmonellosis is an important bacterial disease affecting poultry production and public health, with contaminated feed, water, faecal material, equipment, and human handlers serving as potential sources of transmission. This study investigated the occurrence and molecular characteristics of *Salmonella* isolates recovered from selected poultry farms in Zaria metropolis, Kaduna State, Nigeria. A total of 640 samples comprising 160 faecal-dropping samples, 160 poultry-feed samples, 160 water samples, and 160 hand-swab samples were collected from four selected poultry farms. Samples were subjected to pre-enrichment in peptone water, selective enrichment in Rappaport-Vassiliadis broth, and isolation on Salmonella-Shigella agar. Presumptive isolates were characterized by colonial morphology, Gram staining, and biochemical tests. Genomic DNA was extracted from confirmed isolates and polymerase chain reaction (PCR) assays were used for molecular characterization of *S. Typhimurium* and *S. Pullorum/Gallinarum*. Four *Salmonella*-positive isolates were recovered from the 640 samples, representing an overall prevalence of 0.63%. Molecular characterization identified one isolate as *S. Typhimurium*, while three isolates produced the 182-bp *flhB* amplicon characteristic of the *S. Pullorum/Gallinarum* group. The low prevalence observed in the selected farms does not exclude the potential public-health and veterinary importance of the isolates detected. The findings highlight the need for continued microbiological surveillance, improved farm biosecurity, hygienic handling of feed and water, and molecular monitoring of *Salmonella* in poultry production systems.

Keywords: *Salmonella*, molecular characterization, *Salmonella Typhimurium*, *Salmonella Pullorum/Gallinarum*, poultry, PCR, Zaria

1. Introduction

Salmonellosis is a bacterial infection caused by members of the genus *Salmonella* and is an important foodborne disease affecting humans and animals. Transmission commonly occurs through ingestion of food or water contaminated with animal or human faecal material. Poultry meat, eggs, and their products are recognized as important vehicles for transmission. Clinical manifestations of salmonellosis may include diarrhoea, vomiting, fever, and abdominal pain, with symptoms commonly developing within hours to days following ingestion of contaminated food (Al-Jurayyan et al., 2004).

Salmonella is a major foodborne pathogen worldwide and contributes substantially to morbidity in humans and economic losses in animal production. *Salmonella enterica* comprises numerous serovars, including typhoidal and nontyphoidal groups. Typhoidal salmonellosis is principally associated with *S. Typhi* and *S. Paratyphi*, whereas nontyphoidal salmonellosis is commonly associated with serovars such as *S. Typhimurium* and *S. Enteritidis*. Nontyphoidal *Salmonella* is widely distributed globally and has been reported in different parts of Africa and Nigeria (Kariuki et al., 2006; Mas'ud & Tijjani, 2015).

The genus *Salmonella* currently consists principally of *S. enterica* and *S. bongori*. *S. enterica* is divided into several subspecies, with *S. enterica* subsp. *enterica* being the most important subspecies associated with human and animal infections. Numerous *Salmonella* serovars have been isolated from poultry, poultry products, and poultry production environments (Grimont & Weill, 2007; Uzzau et al., 2000).

Poultry are important reservoirs of *Salmonella*. Infections may result in mortality, reduced productivity, decreased egg production, and considerable economic losses. *S. Pullorum* and *S. Gallinarum* are particularly important host-adapted pathogens of poultry and are associated with pullorum disease and fowl typhoid, respectively. These organisms can persist within poultry production systems and create challenges for disease control (Agbaje et al., 2010; Xiong et al., 2016).

The transmission of *Salmonella* within poultry farms may occur through contaminated feed and feed ingredients, water, equipment, personnel, rodents, and hatchery-related activities. Poor hygiene and inadequate biosecurity can facilitate the maintenance and spread of the organism within poultry production systems (Enabulele et al., 2010; Musa et al., 2014).

Studies conducted in different parts of Nigeria have reported the occurrence of *Salmonella* in poultry, poultry products, poultry environments, and poultry workers. Agada et al. (2014), for example, reported a prevalence of 10.9% among samples obtained from commercial poultry and poultry farm handlers in Jos, Plateau State, and identified several serovars, including *S. Gallinarum*, *S. Typhimurium*, *S. Typhi*, *S. Pullorum*, *S. Enteritidis*, and *S. Paratyphi A*. Fashae et al. (2010) also reported several *Salmonella* serovars among chickens in Ibadan, with *S. Virchow* predominating among the chicken isolates.

Although previous studies have documented *Salmonella* in poultry production systems in Nigeria, information on the molecular characteristics of isolates obtained from different potential sources within poultry farms in Zaria remains limited. Molecular characterization provides an additional means of identifying selected *Salmonella* serovars and can complement conventional microbiological techniques. In particular, the *flhB*-based PCR assay developed by Xiong et al. (2016) provides a molecular approach for detecting the *S. Pullorum/Gallinarum* group, while target-specific PCR has been used for identifying *S. Typhimurium* (Ranjbar et al., 2017).

Therefore, this study aimed to determine the occurrence and molecular characteristics of

Salmonella isolates recovered from faecal droppings, poultry feed, water, and hand swabs collected from selected poultry farms in Zaria metropolis, Kaduna State, Nigeria.

2. Materials and Methods

2.1 Study Area

The study was conducted in Zaria metropolis, Kaduna State, Nigeria. Zaria is located in the northern part of Nigeria and is characterized by a savanna ecological environment. The poultry farms investigated were located in Zaria, Samaru, Palladan, and Tudun Wada.

The study area supports extensive agricultural and poultry production activities, making surveillance of foodborne bacterial pathogens relevant to animal health and public health.

2.2 Study Design and Sample Size

A cross-sectional sampling design was used. A total of 640 samples were collected from four selected poultry farms. Each farm contributed 160 samples comprising 40 faecal-dropping samples, 40 poultry-feed samples, 40 water samples, and 40 hand-swab samples.

The four farms were selected from poultry farms operating within the study area. The original study records indicate that the farms were selected randomly.

2.3 Sample Collection

Samples were collected from the selected poultry farms using sterile containers and swab materials appropriate for the different sample types.

A total of 160 faecal-dropping samples, 160 feed samples, 160 water samples, and 160 hand-swab samples were collected. For faecal samples, 25 g of material was aseptically transferred into 225 mL of peptone water. Poultry-feed samples were collected in 25-g portions, while water samples were collected in 25-mL portions. Hand swabs were collected from poultry handlers using sterile swabs. Samples were appropriately labelled and transported for laboratory analysis.

2.4 Pre-enrichment and Selective Enrichment

For pre-enrichment, 25 g of faecal material was inoculated into 225 mL of peptone water and incubated at 37°C for 24 h. Feed, water, and hand-swab samples were processed using the same general enrichment approach as appropriate to the sample type.

Following pre-enrichment, 1 mL of each enriched sample was transferred into 9 mL of Rappaport-Vassiliadis broth for selective enrichment. The inoculated broth was incubated for 24 h.

2.5 Isolation of *Salmonella*

Following selective enrichment, a loopful of each culture was streaked onto Salmonella-Shigella agar using a sterile wire loop. The plates were incubated for 24 h. Presumptive *Salmonella* colonies were identified based on their characteristic colonial morphology, including colourless colonies with black centres where hydrogen sulphide production was evident.

Presumptive isolates were subcultured onto nutrient agar slants and maintained for further characterization.

2.6 Conventional Identification of *Salmonella* Isolates

Presumptive *Salmonella* isolates were examined by Gram staining and characterized using standard biochemical tests. The biochemical tests included triple sugar iron agar reaction, urease test, motility test, indole test, methyl red-Voges-Proskauer tests, and citrate utilization test.

The identification procedures followed standard bacteriological methods described by Cowan and Steel (2003).

2.7 Genomic DNA Extraction

Three millilitres of an overnight culture of each presumptive *Salmonella* isolate grown in Luria-Bertani broth were centrifuged at 9,000 rpm for 10 min. Genomic DNA was extracted using a commercial DNA extraction kit (Roche, Germany) according to the manufacturer's instructions.

The extracted DNA was transferred into clean tubes and stored at −20°C until required for PCR analysis.

2.8 Molecular Identification of *Salmonella* Typhimurium

PCR was used to identify *S. Typhimurium* using the STM0159 target described by Ranjbar et al. (2017). The PCR mixture had a final volume of 25 µL and contained 1× PCR buffer, 1 mM $MgCl_2$, 1 U Taq DNA polymerase, 200 µM dNTPs, 0.5 µM of each primer, and 2.5 µL of DNA template.

The PCR cycling conditions consisted of an initial denaturation at 95°C for 5 min, followed by 30 cycles of denaturation at 95°C for 60 s, annealing at 57°C for 60 s, and extension at 72°C for 5 min, followed by a final extension at 72°C for 10 min.

The amplified products were separated by electrophoresis on 1.5% agarose gel, stained with ethidium bromide, and visualized using a UV transilluminator.

The STM0159 primer pair produces a 224-bp amplicon for *S. Typhimurium* (Ranjbar et al., 2017).

2.9 Molecular Detection of *Salmonella* Pullorum/Gallinarum

The *S. Pullorum/Gallinarum* group was detected using the *flhB*-target PCR method described by Xiong et al. (2016).

The PCR reaction was performed in a final volume of 25 µL containing approximately 100 ng genomic DNA, 1 U Taq DNA polymerase, 1× PCR buffer, 200 µM of each dNTP, and 0.4 µM of each *flhB* primer.

PCR amplification consisted of an initial denaturation at 95°C for 5 min, followed by 30 cycles of denaturation at 95°C for 45 s, annealing at 59°C for 45 s, and extension at 72°C for 1 min. A final extension was performed at 72°C for 10 min.

The amplified products were separated by electrophoresis on 1% agarose gel in 1× TAE buffer.

The *flhB* assay developed by Xiong et al. (2016) produces a characteristic 182-bp product for the *S. Pullorum/Gallinarum* group. Importantly, this assay identifies the *S. Pullorum/Gallinarum* group and does not, by itself, distinguish *S. Pullorum* from *S. Gallinarum*.

2.10 Primer Sequences

Table 1

Primers Used for Molecular Characterization of Selected *Salmonella* Isolates

Target organism/group	Target gene	Primer	Sequence (5′–3′)	Amplicon size
S. Typhimurium	STM0159	Forward	ATGATGCCTTTTGCTGCTTT	224 bp
S. Typhimurium	STM0159	Reverse	TCCCAGCTCATCCAAAAA	224 bp
S. Pullorum/Gallinarum	*flhB*	Forward	TTCGCGACGAATTTAAAGAGAGCGAAG	182 bp

Target organism/group	Target gene	Primer	Sequence (5′–3′)	Amplicon size
S. Pullorum/Gallinarum	*flhB*	Reverse	CAGCGTTTAAGCTGCCAGACCCAGGCC	182 bp

Note. The *S. Typhimurium* primers were adapted from Ranjbar et al. (2017), and the *S. Pullorum/Gallinarum flhB* primers were from Xiong et al. (2016).

2.11 Data Analysis

The overall prevalence of *Salmonella* was calculated as the proportion of positive samples relative to the total number of samples examined:

Prevalence (%) = (Number of positive samples / Total number of samples examined) × 100

Descriptive analysis was used to summarize the distribution of *Salmonella*-positive samples and molecularly characterized isolates.

3. Results

3.1 Overall Occurrence of *Salmonella*

A total of 640 samples were examined from four selected poultry farms. Four samples were positive for *Salmonella*, representing an overall prevalence of 0.63%.

Table 2

Overall occurrence of *Salmonella* in samples collected from selected poultry farms

Sample status	Number	Percentage (%)
Salmonella-positive samples	4	0.63
Salmonella-negative samples	636	99.38
Total	**640**	**100.00**

The low overall prevalence indicates that *Salmonella* was detected in a small proportion of the samples examined.

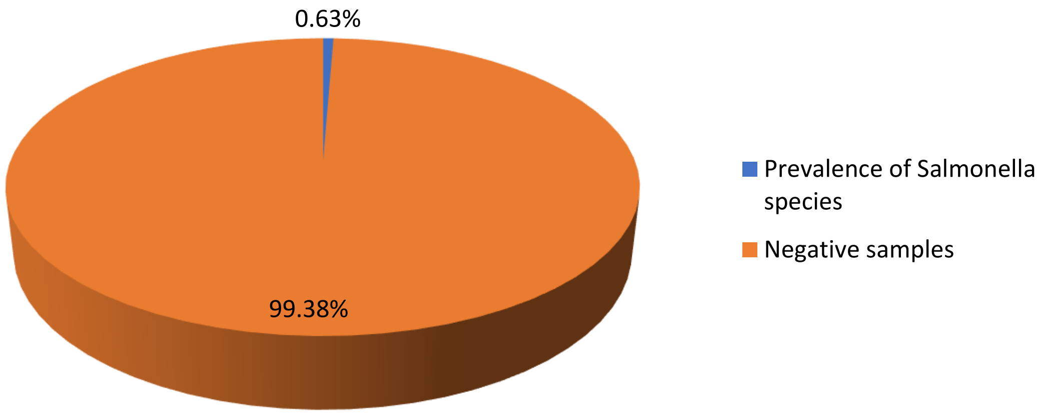


Figure 1: Overall prevalence of Salmonella species in Zaria metropolis

3.2 Distribution of Molecularly Characterized Isolates

Four *Salmonella*-positive isolates were subjected to molecular characterization. Three isolates produced the characteristic 182-bp amplicon associated with the *S. Pullorum/Gallinarum* group, whereas one isolate produced the 224-bp amplicon associated with *S. Typhimuriu*

Table 3

Molecular characterization of *Salmonella* isolates

Isolate	Source	Molecular identification	Amplicon size
PS1	Hand swab	*S. Pullorum/Gallinarum*	182 bp
PW3	Water	*S. Pullorum/Gallinarum*	182 bp
ZF3	Feed	*S. Typhimurium*	224 bp
PW1	Water	*S. Pullorum/Gallinarum*	182 bp

The molecular findings indicate that the *S. Pullorum/Gallinarum* group accounted for three of the four isolates (75%), while *S. Typhimurium* accounted for one isolate (25%).

3.3 PCR Products

The PCR products obtained from the isolates were visualized by agarose gel electrophoresis. The *S. Typhimurium* assay produced a 224-bp band, while the *flhB*-based assay produced a characteristic 182-bp band for isolates belonging to the *S. Pullorum/Gallinarum* group.

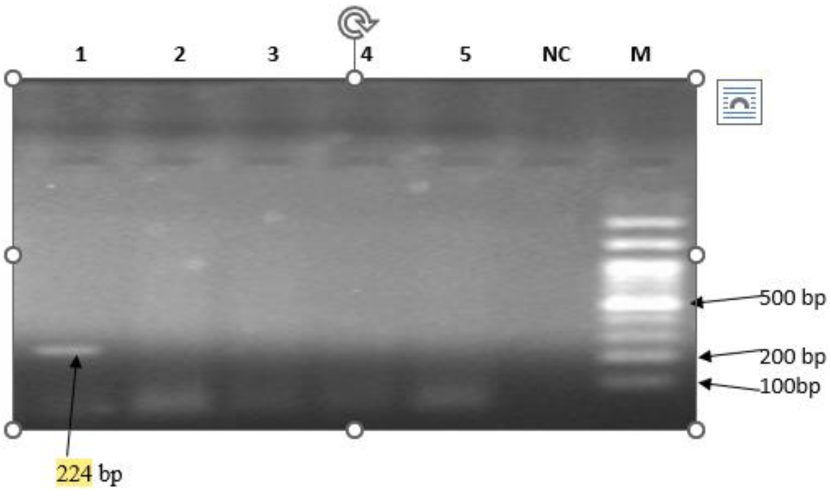


Plate I: Gel electrophoresis result for the detection of *Salmonella* Typhimurium. (Lane M: 100 bp molecular marker, lane 1 to 5 are *Salmonella* isolates while line 6 (NC) is the negative control. Lanes 1 show bands corresponding to 224 bp for *S.* Typhimurium)

Figure 1. Agarose gel electrophoresis showing the 224-bp PCR product associated with *S. Typhimurium*. Lane M represents the molecular-size marker; lanes containing the isolates represent the tested samples, and NC represents the negative control.

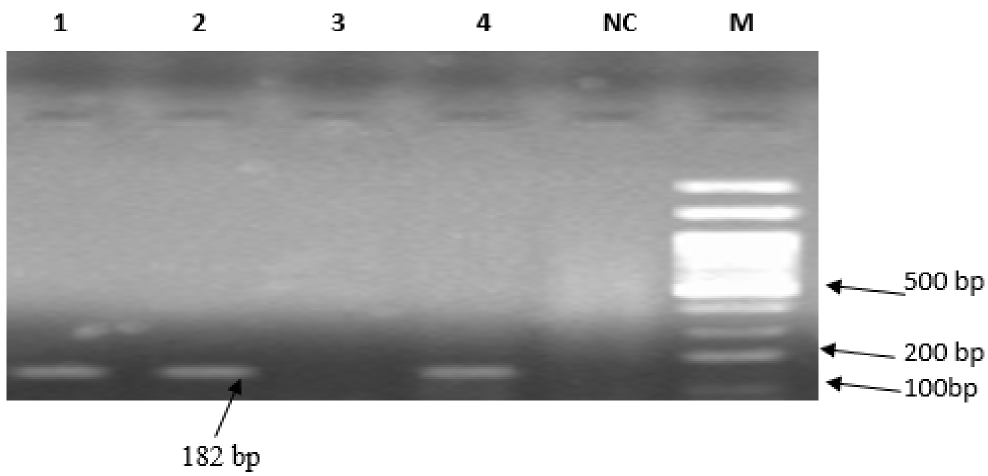


Plate II: Gel electrophoresis result for the detection of Salmonella serotypes (*S.* Gallinarun and *S.* Pullorum). (Lane M: 100 bp molecular marker, lane 1 to 4 are *Salmonella* isolates while line 5 (NC) is the negative control. Lanes 1,2 and 4 show bands corresponding to 182 bp for *S.* Gallinarun / *S.* Pullorum)

Figure 2. Agarose gel electrophoresis showing the 182-bp PCR product associated with the *S. Pullorum/Gallinarum* group. Lane M represents the molecular-size marker; lanes containing the isolates represent the tested samples, and NC represents the negative control.

4. Discussion

The present study detected *Salmonella* in four of 640 samples examined, giving an overall prevalence of 0.63%. This prevalence is lower than values reported in several previous investigations conducted in Nigeria and elsewhere. Agada et al. (2014), for example, reported a prevalence of 10.9% among samples obtained from commercial poultry and poultry farm handlers in Jos, Plateau State. Similarly, other investigations have documented the occurrence of *Salmonella* in poultry production environments and poultry products in Nigeria.

The lower prevalence observed in the present study may reflect differences in sampling locations, sample types, farm-management practices, sampling periods, laboratory methods, or the characteristics of the farms examined. However, because detailed information on antibiotic-use practices, farm biosecurity, flock characteristics, and management systems was not systematically collected in the present study, the low prevalence cannot be directly attributed to any particular management practice.

The detection of *Salmonella* in poultry-associated environmental samples remains important even when prevalence is low. Contaminated water and feed can serve as potential vehicles for dissemination within poultry houses. Similarly, detection from hand swabs indicates the potential role of poultry handlers in mechanical transmission within production environments. Previous studies have identified feed, water, equipment, personnel, rodents, and other environmental sources as potential contributors to *Salmonella* transmission in poultry farms (Agbaje et al., 2010; Enabulele et al., 2010; Musa et al., 2014).

Three of the four molecularly characterized isolates belonged to the *S. Pullorum/Gallinarum* group, while one isolate was identified as *S. Typhimurium*. The occurrence of *S. Pullorum/Gallinarum* is particularly relevant because these host-adapted serovars are associated with poultry diseases and can cause significant production losses. Previous studies have reported *S. Gallinarum* and *S. Pullorum* among poultry-associated *Salmonella* isolates in Nigeria and other countries (Agada et al., 2014; Arora et al., 2015).

The finding of *S. Typhimurium* is also consistent with previous Nigerian reports. Agada et al. (2014) reported *S. Typhimurium* among isolates recovered from commercial poultry and poultry farm handlers in Jos. Fashae et al. (2010) also reported multiple *Salmonella* serovars among chickens and humans in Ibadan, demonstrating the diversity of *Salmonella* circulating within poultry-associated environments in Nigeria.

The predominance of the *S. Pullorum/Gallinarum* group among the four isolates in the present study should, however, be interpreted cautiously. The study examined only four positive isolates, and the sampling involved selected farms rather than all poultry farms in Zaria metropolis. Therefore, the finding should not be interpreted as evidence that *S. Pullorum/Gallinarum* is the predominant *Salmonella* group throughout Zaria.

The molecular approach used in this study provides an advantage over reliance solely on conventional biochemical identification. Xiong et al. (2016) demonstrated that the *flhB*-based PCR assay can specifically detect the *S. Pullorum/Gallinarum* group by producing a 182-bp target amplicon. The authors demonstrated the specificity of the assay against a broad collection of *Salmonella* serovars and non-*Salmonella* organisms.

The present findings should therefore be interpreted in the context of the capability of the molecular assays used. The *flhB* assay identifies the *S. Pullorum/Gallinarum* group but does not independently distinguish *S. Pullorum* from *S. Gallinarum*. Consequently, the three isolates producing the 182-bp product are appropriately reported as *S. Pullorum/Gallinarum* rather than as individually confirmed *S. Pullorum* or *S. Gallinarum*. Molecular assays specifically designed to differentiate the two biovars would be required for definitive discrimination.

The finding of a 224-bp product for the *S. Typhimurium* isolate is consistent with the STM0159 target described by Ranjbar et al. (2017), who developed molecular assays for simultaneous detection of selected *Salmonella enterica* serovars.

The present prevalence of 0.63% is also lower than the 2.7% prevalence reported by Arora et al. (2015) in commercial broiler chicken flocks in Haryana, India. Differences between studies may reflect variations in flock health, environmental conditions, geographical location, sampling procedures, sample sizes, and diagnostic methods.

In contrast, Fashae et al. (2010) reported *S. Virchow* as the predominant serovar among chicken isolates in Ibadan. This differs from the present study, in which the *S. Pullorum/Gallinarum* group was the most frequently detected molecular group. Such differences further demonstrate the geographical and temporal variability of *Salmonella* serovars in poultry populations.

The findings emphasize the importance of continued surveillance of poultry production environments. Even a low prevalence of potentially pathogenic *Salmonella* organisms may have implications for poultry health and food safety because contaminated poultry products or production environments may serve as points of transmission. Regular microbiological monitoring, improved hygiene, appropriate handling of feed and water, and strengthened farm biosecurity remain important components of *Salmonella* control.

5. Conclusion and Recommendations

This study investigated the occurrence and molecular characteristics of *Salmonella* isolates recovered from selected poultry farms in Zaria metropolis. Four *Salmonella*-positive isolates were recovered from 640 samples, representing an overall prevalence of 0.63%. Molecular characterization identified three isolates as belonging to the *S. Pullorum/Gallinarum* group based on the characteristic 182-bp *flhB* PCR product and one isolate as *S. Typhimurium* based on the 224-bp STM0159 PCR product.

The results demonstrate the presence of poultry-associated *Salmonella* in selected farms in Zaria despite the low prevalence observed. Because the *flhB* assay used in this study identifies the *S. Pullorum/Gallinarum* group rather than differentiating the two biovars, the three isolates should not be interpreted as individually confirmed *S. Pullorum* or *S. Gallinarum*. Further molecular characterization using discriminatory assays would be useful for differentiating these two biovars.

The findings support the need for continued *Salmonella* surveillance, good hygienic practices, proper management of feed and water, and effective biosecurity measures in poultry farms.

Recommendations

1. Routine microbiological surveillance of poultry farms should be encouraged to detect *Salmonella* contamination at an early stage.
2. Poultry farmers should strengthen biosecurity measures and maintain hygienic poultry-house environments.
3. Feed and water should be protected from faecal contamination and other potential sources of *Salmonella*.
4. Poultry handlers should maintain appropriate personal hygiene, particularly hand hygiene, during farm operations.
5. Molecular methods should be incorporated into surveillance programmes where resources permit, particularly for characterization of important *Salmonella* serovars.
6. Future studies should use larger sample sizes and include more poultry farms to provide a more representative estimate of *Salmonella* occurrence in Zaria metropolis.
7. Future molecular studies should employ discriminatory assays capable of distinguishing *S. Pullorum* from *S. Gallinarum*.

References

Agada, G. O. A., Abdullahi, I. O., Aminu, M., Odugbo, M., Chollom, S. C., Kumbish, P. R., & Okwori, A. E. J. (2014). Prevalence and antibiotic resistance profile of *Salmonella* isolates from commercial poultry and poultry farm-handlers in Jos, Plateau State, Nigeria. *Microbiology Research Journal International, 4*(4), 462–479. https://doi.org/10.9734/BMRJ/2014/5872

Agbaje, M., Davies, R., Oyekunle, M. A., Ojo, O. E., Fasina, F. O., & Akinduti, P. A. (2010). Observation on the occurrence and transmission pattern of *Salmonella Gallinarum* in commercial poultry farms in Ogun State, South Western Nigeria. *African Journal of Microbiology Research, 4*(9), 796–800.

Al-Jurayyan, A. M., Al-Rasheedi, N. A. M., Mohammad, N., Alnasser, M. M., Mugeiren, A. T., & Abdullahi, S. A. (2004). Childhood bacterial diarrhoea in a regional hospital in Saudi Arabia. *Journal of Tropical Medicine and Hygiene, 97*, 87–90.

Arora, D., Kumar, S., Jindal, N., Narang, G., Kapoor, P. K., & Mahajan, N. K. (2015). Prevalence and epidemiology of *Salmonella enterica* serovar Gallinarum from poultry in some parts of Haryana, India. *Veterinary World, 8*(11), 1300–1304.

Cowan, S. T., & Steel, K. J. (2003). *Cowan and Steel's manual for the identification of medical bacteria* (3rd ed., G. I. Barrow & R. K. A. Feltham, Eds.). Cambridge University Press.

Enabulele, A. S., Amune, P. O., & Aborisade, W. T. (2010). Antibiograms of *Salmonella* isolates from poultry farms in Ovia North East Local Government Area, Edo State, Nigeria. *Agriculture and Biology Journal of North America, 1*(6), 1287–1290.

Fashae, K., Ogunsola, F., Aarestrup, F. M., & Hendriksen, R. S. (2010). Antimicrobial susceptibility and serovars of *Salmonella* from chickens and humans in Ibadan, Nigeria. *Journal of Infection in Developing Countries, 4*(8), 484–494. https://doi.org/10.3855/jidc.909

Garba, M. K., Olonitola, O. S., Yakubu, S. E., & Abdullahi, I. O. (2017). Antimicrobial susceptibility and occurrence of resistance genes among *Salmonella Arizonae* isolated from chicken meat samples in Sokoto metropolis, Sokoto State, Nigeria. *UMYU Journal of Microbiology Research, 2*(2).

Grimont, P. A. D., & Weill, F. X. (2007). *Antigenic formulae of the Salmonella serovars* (9th ed.). WHO Collaborating Centre for Reference and Research on *Salmonella*, Institut Pasteur.

Kariuki, S., Revathi, G., Kariuki, N., Kiiru, J., Mwituria, J., & Hart, C. A. (2006). Characterization of community acquired nontyphoidal *Salmonella* from bacteraemia and diarrhoeal infection in children admitted to hospital in Nairobi, Kenya. *BMC Microbiology, 6*, Article 101.

Mas'ud, A., & Tijjani, M. (2015). Prevalence and multiple antibiotic resistance patterns of *Salmonella* serovars isolated from blood samples of hospitalized patients in Kano, North-West, Nigeria. *IOSR Journal of Pharmacy and Biological Sciences, 10*(2), 125–135.

Muhammed, M., Muhammed, L. U., Ambali, A. G., Mani, A. U., Azard, S., & Barco, L. (2010). Prevalence of *Salmonella* associated with chick mortality at hatching and their susceptibility to antimicrobial agents. *Veterinary Microbiology, 140*, 131–135.

Musa, I. W., Mansur, M. S., Sa'idu, L., Mohammed, B., Kaltungo, B. Y., Lawan, M. K., & Talba, A. M. (2014). Isolation and antibiogram of *Salmonella* species from water and poultry feed in selected commercial farms in Zaria, Nigeria. *Time Journals of Agriculture and Veterinary Sciences, 2*(2), 75–80.

Ogunleye, A. O., Ajuwape, A. T. P., Adetosoye, A. I., & Ohore, O. G. (2006). Pathogenicity of *Salmonella Paratyphi A* in pullets. *Revue d'Élevage et de Médecine Vétérinaire des Pays Tropicaux, 59*, 5–9.

Ranjbar, R., Mortazavi, S. M., Tavana, A. M., Sarshar, M., Najafi, A., & Zanjani, R. S. (2017). Simultaneous molecular detection of *Salmonella enterica* serovars Typhi, Enteritidis, Infantis, and Typhimurium. *Iranian Journal of Public Health, 46*(1), 103–111.

Ricardo, A., & Brazil, S. (2012). Salmonella special: Reducing risks of *Salmonella* infections in poultry. *World Poultry*, 2–6.

Roth, N. (2012). The use of acidifiers in controlling *Salmonella*. *World Poultry*, 1–4.

Uwaezuoke, J. C., Obbloulie, J. N., & Njoku, A. I. (2000). Antibiotics sensitivity patterns of bacterial isolates from poultry feed. *International Journal of Environmental, Health and Human Development, 1*, 23–28.

Uzzau, S., Brown, D. J., Wallis, T., Rubino, S., Leori, G., Bernard, S., Casadesus, J., Platt, D. J., & Olsen, J. E. (2000). Host adapted serotypes of *Salmonella enterica*. *Epidemiology and Infection, 125*, 229–255.

Xiong, D., Song, L., Geng, S., Tao, J., An, S., Pan, Z., & Jiao, X. (2016). One-step PCR detection of *Salmonella Pullorum/Gallinarum* using a novel target: The flagellar biosynthesis gene *flhB*. *Frontiers in Microbiology, 7*, Article 1863. https://doi.org/10.3389/fmicb.2016.01863

Yhiler, N. Y., & Bassey, B. E. (2015). Antimicrobial susceptibility patterns of *Salmonella* species from sources in poultry production settings in Calabar, Cross River State, Nigeria. *American Journal of Health Research, 3*(2), 76–81.

Cyber-Physical Security of Analytical Chemistry and Physics Instrumentation: Vulnerability Assessment and Intelligent Threat Detection

Mary Ninma Esuga-Mopah, Omananyi Muhammed Rabiu & Salihu Abubakar

Department of Science Laboratory Technology, Kogi State Polytechnic, Lokoja

Abstract

The increasing integration of digital technologies, network connectivity, sensors, embedded controllers, cloud platforms, and artificial intelligence into analytical chemistry and physics laboratories has transformed scientific measurement and experimentation. Modern analytical instruments such as spectrometers, chromatographs, mass spectrometers, electrochemical analysers, radiation detectors, digital oscilloscopes, and automated measurement systems increasingly operate as cyber-physical systems (CPS). While connectivity improves automation, remote monitoring, data processing, and collaborative research, it also introduces cybersecurity risks capable of compromising the confidentiality, integrity, and availability of scientific data and measurement processes. A successful cyberattack on an analytical instrument may not only expose information but also manipulate experimental parameters, alter measurements, disrupt instrument operation, or compromise the reliability and reproducibility of scientific results. This paper examines the cyber-physical security of analytical chemistry and physics instrumentation, focusing on vulnerability assessment and intelligent threat detection. A conceptual research framework was developed by integrating principles from analytical chemistry, physics, operational technology security, cyber-physical systems, artificial intelligence, and cybersecurity risk management. The framework categorises vulnerabilities into instrument, communication, software, human, data, and physical layers and proposes a multi-stage intelligent threat detection architecture based on continuous monitoring, behavioural profiling, anomaly detection, and risk scoring. The analysis indicates that conventional information technology security controls alone are insufficient because scientific instruments possess physical processes, measurement constraints, calibration requirements, and safety considerations that must be incorporated into cybersecurity strategies. The paper recommends risk-based security assessment, network segmentation, secure authentication, integrity monitoring, instrument-level logging, anomaly detection, cybersecurity awareness, and integration of laboratory security with established frameworks such as the NIST Cybersecurity Framework 2.0 and NIST guidance for operational technology. The proposed framework provides a foundation for protecting scientific measurement systems and strengthening the integrity and reliability of digitally connected analytical and physics laboratories.

Keywords: analytical chemistry, physics instrumentation, cyber-physical systems, cybersecurity, vulnerability assessment, intelligent threat detection, laboratory security, scientific data integrity

1. Introduction

The transformation of modern laboratories through digitalisation has created an increasingly interconnected environment in which scientific instruments, computers, sensors, embedded controllers, databases, laboratory information management systems, cloud platforms, and communication networks operate as an integrated ecosystem. Analytical chemistry and physics laboratories have particularly benefited from this transformation. Instruments that previously operated as relatively isolated systems can now communicate with computers, institutional networks, cloud applications, external databases, and remote users (Miruna Lucretia Comeaga, 2022).

Analytical chemistry relies heavily on instrumentation for the identification, separation, quantification, and characterisation of chemical substances. Examples include ultraviolet-visible (UV-Vis) spectrophotometers, Fourier-transform infrared (FTIR) spectrometers, nuclear magnetic resonance (NMR) instruments, gas chromatographs (GC), liquid chromatographs (LC), mass spectrometers, atomic absorption spectrometers, inductively coupled plasma systems, electrochemical analysers, and automated titration systems. Physics laboratories similarly depend on digital instrumentation including oscilloscopes, spectrum analysers, radiation detectors, laser systems, digital multimeters, data acquisition systems, temperature and pressure sensors, and imaging systems (Kumat, 2025).

The increasing connectivity of these instruments creates characteristics associated with cyber-physical systems (CPS). A cyber-physical system combines computational components with physical processes through sensing, communication, computation, and control. In laboratory environments, the physical process may involve chemical reactions, temperature, pressure, radiation, electrical signals, optical measurements, fluid flow, or other measurable physical phenomena. The cyber component receives measurements, processes data, stores information, controls instruments, and communicates with other systems (Tyagi & Sreenath, 2021).

The cybersecurity implications of this transformation are significant. The compromise of a laboratory instrument may have consequences beyond the loss of computer files. For example, manipulation of calibration parameters could produce systematically incorrect measurements, while unauthorised alteration of acquisition settings could affect experimental reproducibility. Similarly, malicious modification of a temperature, pressure, voltage, radiation, or optical measurement could lead to erroneous scientific conclusions (Shaik et al., 2025).

The National Institute of Standards and Technology (NIST) recognises that operational technology systems interact directly with the physical environment and therefore require security approaches that consider performance, reliability, safety, and physical consequences (Stouffer et al., 2023). NIST's operational technology guidance specifically includes physical environment monitoring and measurement systems within the broader OT landscape.

The NIST Cybersecurity Framework (CSF) 2.0 provides a flexible approach for organisations to understand, assess, prioritise, and communicate cybersecurity risks. Its applicability extends beyond traditional information technology environments and includes organisations with different levels of cybersecurity maturity (Pascoe et al., 2024).

Similarly, the ISA/IEC 62443 family provides a structured approach to securing industrial automation and control systems by addressing cybersecurity across technology, processes, and organisational responsibilities. The standards emphasise the integration of operational requirements with cybersecurity and process safety.

Despite the growing adoption of digital laboratory instrumentation, cybersecurity research has focused predominantly on conventional information systems, industrial control systems, healthcare systems, and Internet of Things devices. Comparatively less attention has been devoted to the security of scientific measurement instruments and the integrity of analytical results.

The objective of this paper is therefore to develop a conceptual framework for assessing vulnerabilities and detecting cyber threats in analytical chemistry and physics instrumentation. Specifically, the study aims to:

1. identify major cybersecurity vulnerabilities associated with digitally connected analytical chemistry and physics instruments;
2. examine the potential consequences of cyberattacks on scientific measurements and laboratory operations;
3. develop an intelligent threat detection framework suitable for cyber-physical laboratory environments; and
4. propose security measures for improving the confidentiality, integrity, availability, authenticity, and reliability of scientific measurement systems.

2. Literature Review

2.1 Cyber-Physical Systems and Scientific Instrumentation

Cyber-physical systems integrate computational processes with physical processes through sensing, communication, computation, and control. Unlike conventional information systems, CPS environments combine digital and physical components. Consequently, cybersecurity incidents can produce physical consequences and measurement errors (Blessing & Kiu Publication Extension, 2024).

Scientific instruments increasingly exhibit these characteristics. A spectrophotometer, for example, may contain optical sensors, analogue-to-digital converters, embedded processors, firmware, communication interfaces, control software, and a workstation. A chromatographic system similarly combines pumps, valves, detectors, temperature controllers, sensors, software, and data storage.

The integration of these components creates several potential attack surfaces. An attacker may target the network interface, instrument software, firmware, operating system, user credentials, communication protocols, removable media, or connected workstation. The risk becomes greater when instruments use outdated operating systems or software that cannot easily be patched because of vendor restrictions, compatibility requirements, or validation constraints.

NIST's guidance on operational technology security notes that OT systems differ from conventional information technology because their security controls must account for unique performance, reliability, and safety requirements (Stouffer et al., 2023). These characteristics are equally relevant to advanced laboratory instrumentation where uninterrupted operation, measurement accuracy, calibration, and physical safety are important.

2.2 Analytical Chemistry Instrumentation as a Cyber-Physical Environment

Analytical chemistry instruments generate large quantities of digital information. A typical analytical workflow can involve sample identification, instrument configuration, calibration, measurement acquisition, signal processing, interpretation, storage, and reporting.

Each stage may introduce cybersecurity vulnerabilities. For instance, unauthorised access to instrument software could allow alteration of acquisition parameters. Compromise of a data-processing workstation could allow modification of chromatograms or spectra. Manipulation of calibration data could create systematic measurement bias without necessarily producing an obvious indication of cyberattack.

Data integrity is particularly important in analytical chemistry because the credibility of an analytical result depends not only on the measurement itself but also on traceability, calibration, quality control, sample identification, and appropriate data processing (Vicente et al., 2026).

2.3 Physics Instrumentation and Cybersecurity

Physics instrumentation presents similar risks. Modern physics laboratories employ highly sensitive instruments for measuring electrical, optical, mechanical, thermal, nuclear, and electromagnetic phenomena. Many instruments incorporate microprocessors, embedded operating systems, network interfaces, USB connectivity, remote administration capabilities, and automated data acquisition (Ismail & Abdulrazzak, 2019).

An attacker who gains access to a measurement system could manipulate measurement parameters, introduce false data, disrupt acquisition, or modify control signals. In experiments involving high voltage, lasers, radiation, cryogenic systems, vacuum systems, or high-temperature equipment, cybersecurity incidents may additionally create physical safety risks.

The security of such systems therefore requires an approach that combines cybersecurity with physical safety, equipment reliability, measurement science, and laboratory risk management.

2.4 Vulnerabilities in Cyber-Physical Laboratory Systems

The vulnerabilities of digitally connected scientific instrumentation can be grouped into six major categories.

2.4.1 Instrument-Level Vulnerabilities

These include insecure firmware, outdated operating systems, default credentials, unsupported software, exposed communication ports, inadequate access controls, and insufficient logging.

2.4.2 Network Vulnerabilities

Laboratory instruments connected directly to institutional networks may become exposed to network-based attacks. Poor segmentation can enable attackers who compromise an ordinary workstation to move laterally toward instrument systems.

2.4.3 Software Vulnerabilities

Instrument control software may contain unpatched vulnerabilities, insecure authentication mechanisms, inadequate input validation, or weak mechanisms for protecting configuration files and measurement records.

2.4.4 Human Vulnerabilities

Laboratory personnel may unintentionally introduce threats through weak passwords, phishing, unauthorised software installation, use of infected removable storage devices, or failure to follow established cybersecurity procedures.

2.4.5 Data Vulnerabilities

Scientific data may be altered, deleted, copied, or manipulated during acquisition, transmission, processing, storage, or reporting. The consequences can include loss of reproducibility and compromised research integrity.

2.4.6 Physical Vulnerabilities

Unauthorised physical access to an instrument may enable manipulation of controls, installation of malicious devices, theft of storage media, or connection of unauthorised equipment.

2.5 Intelligent Threat Detection

Traditional signature-based security mechanisms are useful for detecting known threats but may be inadequate against novel or previously unseen attacks. Intelligent threat detection approaches can instead establish a baseline of normal instrument behaviour and identify deviations from that baseline (Ahmed et al., 2025).

Machine learning can be applied to network traffic, login patterns, system events, instrument parameters, data-access behaviour, and sensor measurements. Anomalies may indicate compromised credentials, malicious configuration changes, unusual network communication, abnormal data transfer, or manipulation of instrument operation.

However, intelligent detection in laboratory environments requires domain knowledge. Not every unusual measurement represents a cyberattack. Scientific experiments naturally generate variations due to sample properties, environmental conditions, instrument drift, calibration changes, or experimental design. Consequently, cybersecurity detection systems should combine cyber indicators with scientific and physical context.

2.6 Cybersecurity Frameworks

NIST CSF 2.0 provides a general framework for managing cybersecurity risks and is organised around the functions Govern, Identify, Protect, Detect, Respond, and Recover (Pascoe et al., 2024).

NIST SP 800-82 Rev. 3 provides guidance for securing operational technology systems and addresses threats, vulnerabilities, system architectures, and countermeasures while recognising the unique requirements of OT environments (Stouffer et al., 2023).

The ISA/IEC 62443 standards similarly provide cybersecurity requirements and processes for industrial automation and control systems and emphasise a holistic relationship between information technology, operational technology, and process safety (International Society of Automation, 2024).

These frameworks provide useful foundations for laboratory cybersecurity but require adaptation to the specific characteristics of analytical chemistry and physics instrumentation.

3. Methodology

3.1 Research Design

This study adopted a design-oriented and conceptual research methodology. The approach integrates concepts from analytical chemistry, physics instrumentation, cyber-physical systems, cybersecurity, artificial intelligence, and operational technology security.

The study did not claim experimental attack results or laboratory measurements that were not actually conducted. Instead, an analytical framework was developed to identify vulnerabilities and establish an intelligent threat detection architecture for digitally connected scientific instruments.

3.2 System Modelling

A generic cyber-physical laboratory instrumentation architecture was developed comprising six layers:

1. **Physical measurement layer** – samples, chemical processes, optical systems, electrical systems, thermal systems, radiation sources, and other physical processes.
2. **Sensor and actuator layer** – detectors, sensors, motors, valves, pumps, temperature controllers, voltage controllers, and other interfaces.
3. **Embedded instrumentation layer** – microcontrollers, firmware, instrument processors, and internal control systems.
4. **Communication layer** – Ethernet, Wi-Fi, USB, serial interfaces, Bluetooth, and other communication mechanisms.

5. **Application and data layer** – instrument control software, databases, laboratory information systems, data-processing applications, and cloud platforms.
6. **Human and governance layer** – analysts, researchers, technicians, administrators, cybersecurity personnel, policies, procedures, and access-control mechanisms.

This layered architecture permits vulnerabilities to be evaluated systematically rather than treating the laboratory as a conventional computer network.

3.3 Vulnerability Assessment Model

A vulnerability assessment model was developed using five principal dimensions:

- **Exposure (E):** degree to which an instrument or component is accessible to unauthorised entities;
- **Exploitability (X):** difficulty of exploiting the identified weakness;
- **Impact (I):** potential effect on confidentiality, integrity, availability, safety, and scientific validity;
- **Detectability (D):** likelihood that malicious activity can be identified promptly; and
- **Recovery difficulty (R):** difficulty associated with restoring secure and reliable operation.

A conceptual risk score may be represented as:

$$\textbf{Risk Score} = E \times X \times I \times R$$

where each parameter is assigned a standardised score from 1 to 5.

Higher scores indicate greater cybersecurity priority. The model can subsequently be adapted to institutional risk-management requirements.

3.4 Intelligent Threat Detection Architecture

The proposed detection architecture consists of five stages.

Stage 1: Data Collection

Security-relevant information is collected from instrument logs, operating systems, network traffic, authentication records, configuration changes, data-access events, and relevant sensor measurements.

Stage 2: Feature Extraction

Relevant features are extracted, including:

- login frequency;
- source and destination addresses;
- communication frequency;
- unusual ports;
- configuration changes;
- instrument operating states;
- measurement patterns;
- data-transfer volume;
- failed authentication attempts; and
- abnormal process behaviour.

Stage 3: Behavioural Profiling

Normal laboratory behaviour is established using historical operational data. The baseline should account for scheduled maintenance, calibration, routine experiments, instrument shutdowns, and normal variations in measurement conditions.

Stage 4: Anomaly Detection

Anomaly detection algorithms identify observations that significantly deviate from established patterns. Depending on data availability, statistical methods, isolation-based algorithms, clustering, autoencoders, or other machine-learning techniques may be applied.

Stage 5: Risk Classification and Response

Detected anomalies are assigned risk levels. Low-risk events may be logged for review, medium-risk events may trigger alerts, while high-risk events may require isolation of the affected system and investigation by laboratory and cybersecurity personnel.

3.5 Evaluation Criteria

The proposed framework was evaluated conceptually using five criteria:

1. ability to identify instrument vulnerabilities;
2. ability to protect measurement integrity;
3. suitability for detecting abnormal behaviour;
4. compatibility with laboratory operations; and
5. alignment with established cybersecurity frameworks.

4. Results and Discussion

4.1 Identified Vulnerability Landscape

The analysis indicates that cyber-physical laboratory instrumentation has a broader attack surface than conventional standalone laboratory equipment. Connectivity introduces potential entry points through networks, computers, removable devices, remote-access applications, cloud services, and software updates.

The most critical vulnerability category is expected to be **data and measurement integrity** because manipulation of scientific data may not immediately produce an obvious operational failure. An instrument can continue functioning normally while producing compromised results.

This creates an important distinction between conventional cybersecurity and scientific-instrument cybersecurity. In a conventional information system, unauthorised modification of a file may be the principal concern. In a scientific laboratory, modification of a measurement may undermine an entire experiment while leaving the instrument apparently functional.

4.2 Cybersecurity Risks to Analytical Chemistry

Analytical instruments frequently depend on software for instrument control, calibration, signal processing, peak identification, quantitative analysis, and report generation. Consequently, compromise at any stage can influence the final analytical result.

For example, unauthorised modification of calibration parameters could produce systematic bias. Manipulation of chromatographic processing parameters could influence peak integration. Alteration of spectral-processing settings could affect interpretation. Similarly, manipulation of sample identification information could result in incorrect association between a measurement and a specimen.

The implication is that cybersecurity controls should extend beyond the workstation and network to include the integrity of instrument configurations, calibration records, analytical methods, and processed data.

4.3 Cybersecurity Risks to Physics Instrumentation

Physics instrumentation presents additional concerns because measurements often depend on precise physical conditions. An unauthorised modification to temperature, pressure, voltage, frequency, timing, optical alignment, or detector settings could affect experimental outcomes.

In some environments, cyber manipulation could also create physical hazards. Consequently, the cybersecurity architecture should incorporate safety-related controls and fail-safe mechanisms.

NIST's OT security guidance emphasises the importance of addressing cybersecurity while maintaining the performance, reliability, and safety requirements of systems interacting with the physical environment (Stouffer et al., 2023).

4.4 Intelligent Detection and Measurement Integrity

The proposed intelligent detection framework provides an opportunity to detect attacks that may not be identified through conventional antivirus or firewall mechanisms.

For example, an authentication anomaly combined with an unexpected instrument configuration change and unusual outbound network traffic should generate a higher risk score than any of these events considered independently.

Similarly, scientific measurements can provide an additional source of cybersecurity intelligence. If a sensor suddenly produces values inconsistent with established physical constraints while no corresponding experimental change has occurred, the event may warrant investigation.

However, intelligent detection must distinguish between legitimate experimental variability and malicious behaviour. This is particularly important in research laboratories where experimental conditions may intentionally change.

The detection model should therefore use **context-aware anomaly detection** rather than relying solely on fixed thresholds.

4.5 Proposed Security Architecture

The analysis supports a defence-in-depth architecture consisting of:

- network segmentation;
- instrument-specific access control;
- multi-factor authentication where technically feasible;
- secure configuration management;
- firmware and software integrity verification;
- controlled removable media;
- encrypted communication where supported;
- centralised logging;
- continuous anomaly monitoring;
- regular vulnerability assessment;
- secure backup of configurations and data;
- incident response procedures; and
- periodic cybersecurity training.

Network segmentation is particularly important. Instruments should not automatically be placed on the same unrestricted network as ordinary office computers. Segmentation can limit lateral movement if another device is compromised.

4.6 Alignment with NIST CSF 2.0

The proposed framework can be mapped to the six functions of NIST CSF 2.0.

NIST CSF 2.0 Function	Application to Laboratory Instrumentation
Govern	Establish laboratory cybersecurity policies, responsibilities, and risk governance
Identify	Inventory instruments, software, users, data, communication paths, and vulnerabilities
Protect	Implement authentication, segmentation, access control, backups, and secure configurations
Detect	Monitor logs, network traffic, instrument behaviour, and measurement anomalies
Respond	Contain compromised instruments, investigate incidents, and protect scientific data
Recover	Restore secure configurations, validate instrument performance, and recover trusted data

NIST describes CSF 2.0 as a framework for managing cybersecurity risk that can be applied across organisations and sectors rather than being restricted to a particular technology or industry (Pascoe et al., 2024).

This makes it suitable as a governance foundation for laboratory cybersecurity, provided that laboratory-specific measurement and safety requirements are incorporated.

4.7 Implications for Scientific Data Integrity

Scientific data integrity should be treated as a cybersecurity objective rather than merely an issue of research methodology. The integrity of a result depends on the authenticity and reliability of the complete measurement chain.

This includes:

sample → instrument → sensor → acquisition software → processing → database → analysis → report.

A weakness at any point may compromise the final result.

Therefore, laboratory cybersecurity programmes should incorporate mechanisms for data provenance, audit trails, configuration integrity, access control, and secure backups. Where appropriate, cryptographic hashing can be used to detect unauthorised changes to critical files and records.

4.8 Implications for Laboratories in Developing Research Environments

In many developing research environments, laboratory cybersecurity may receive less attention than instrument acquisition and maintenance. However, the increasing use of network-enabled instruments makes cybersecurity an important component of laboratory management.

Institutions should therefore include cybersecurity requirements when procuring scientific instruments. Procurement specifications should address supported operating systems, patching mechanisms, authentication, logging, network security, vendor support, firmware updates, data export, backup, and vulnerability disclosure.

This is particularly important because some scientific instruments have long operational lifetimes and may continue to use legacy software after vendor support has declined.

5. Conclusions and Recommendations

5.1 Conclusion

The increasing digitalisation and connectivity of analytical chemistry and physics instrumentation has transformed scientific laboratories into cyber-physical environments. While network connectivity improves automation, remote monitoring, data management, and research collaboration, it also introduces cybersecurity vulnerabilities that can affect not only information systems but also physical processes and the integrity of scientific measurements.

The study established that vulnerabilities may occur at the physical, sensor, embedded instrumentation, communication, software, data, and human layers. Of particular concern is the possibility of attacks that manipulate scientific measurements without causing obvious instrument failure.

The proposed intelligent threat detection framework combines vulnerability assessment, behavioural profiling, anomaly detection, contextual analysis, and risk-based response. Its principal contribution is the integration of cybersecurity monitoring with the scientific and physical characteristics of laboratory instrumentation.

The study further demonstrates that established cybersecurity frameworks such as NIST CSF 2.0 and NIST OT security guidance provide useful foundations but should be adapted to address instrument calibration, measurement uncertainty, data provenance, experimental variability, safety, and scientific reproducibility. NIST's current OT guidance explicitly recognises systems involved in physical-environment monitoring and measurement as part of the OT security landscape.

Cybersecurity in analytical chemistry and physics should therefore be considered an integral component of scientific quality assurance rather than an independent information-technology concern.

5.2 Recommendations

Based on the analysis, the following recommendations are proposed:

1. **Establish laboratory cybersecurity policies:** Research institutions should develop specific cybersecurity policies for scientific instruments and laboratory information systems.
2. **Maintain an instrument asset inventory:** Every network-enabled instrument should be documented, including hardware, software, firmware, communication interfaces, users, data flows, and vendor support status.
3. **Conduct regular vulnerability assessments:** Laboratories should periodically evaluate instrument configurations, software, network exposure, authentication mechanisms, and access controls.
4. **Implement network segmentation:** Scientific instruments should be isolated from general-purpose office networks where appropriate, with controlled communication between instrument networks and institutional systems.
5. **Deploy intelligent monitoring:** Institutions should implement behavioural and anomaly-based monitoring capable of detecting unusual network, user, configuration, and measurement activity.
6. **Protect scientific data integrity:** Critical measurement data, calibration records, analytical methods, and instrument configurations should be protected through access control, audit trails, cryptographic integrity mechanisms, and secure backups.
7. **Strengthen authentication:** Default credentials should be eliminated and strong authentication should be implemented according to the technical capabilities of each instrument.
8. **Include cybersecurity in procurement:** New laboratory instruments should be

evaluated for cybersecurity capabilities before purchase.

9. **Train laboratory personnel:** Scientists, laboratory technologists, technicians, students, and administrators should receive regular cybersecurity awareness training.

10. **Develop incident-response procedures:** Laboratories should establish procedures for isolating compromised instruments, preserving evidence, validating instrument performance, and recovering trusted data.

11. **Integrate cybersecurity with laboratory quality management:** Cybersecurity controls should complement existing calibration, validation, quality assurance, safety, and research-integrity procedures.

12. **Conduct empirical validation:** Future studies should implement the proposed framework in real analytical chemistry and physics laboratories using authorised test environments and benchmark datasets. Such studies should measure detection accuracy, false-positive rates, response time, computational overhead, and the effect of cybersecurity controls on instrument performance.

References

Ahmed, U., Nazir, M., Sarwar, A., Ali, T., Aggoune, E.-H. M., Shahzad, T., & Khan, M. A. (2025). Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-025-85866-7

Blessing, N. J., & Kiu Publication Extension. (2024). *Cyber-physical systems: Integrating computing with physical processes*. *3*(2), 49–52. https://www.researchgate.net/publication/383874108_Cyber-Physical_Systems_Integrating_Computing_with_Physical_Processes

International Society of Automation. (2025). *ISA/IEC 62443 series of standards: Security for industrial automation and control systems*. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards (isa.org)

International Society of Automation. (2024). ISA/IEC 62443 Series of Standards - ISA. In *isa.org*. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

Ismail, A. A., & Abdulrazzak, F. H. (2019). Laboratory instruments classification and risks use with safety for less mistakes. *Journal of Physics Conference Series*, *1294*(5), 052077–052077. https://doi.org/10.1088/1742-6596/1294/5/052077

Kumat, D. (2025). Spectroscopic techniques in chemical analysis: A review of emerging trends. *Indian Journal of Pharmaceutical Chemistry and Analytical Techniques*, *1*(3), 55–70. https://doi.org/10.64062/ijpcat.vol1.issue3.5

Miruna Lucretia Comeaga. (2022). Digital transformation of the laboratories. *IOP Conference Series: Materials Science and Engineering*, *1268*(1), 012001–012001. https://doi.org/10.1088/1757-899x/1268/1/012001

Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Paper 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29 (NIST)

Shaik, A. K., Mohammadi, A., & Malik, H. (2025). A systematic review of sensor vulnerabilities and cyber-physical threats in industrial robotic systems. *IET Cyber-Physical Systems Theory & Applications*, *10*(1). https://doi.org/10.1049/cps2.70023

Stouffer, K., Pease, M., Tang, C. Y., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). *Guide to operational technology (OT) security* (NIST Special Publication 800-82 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3 (NIST Computer Security Resource Center)

Stouffer, K. A., Pillitteri, V. Y., Lightman, S., Abrams, M., & Hahn, A. (2015). *Guide to industrial control systems (ICS) security* (NIST Special Publication 800-82 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r2 (NIST Computer Security Resource Center)

Tyagi, A. K., & Sreenath, N. (2021). Cyber physical systems: Analyses, challenges and possible solutions. *Internet of Things and Cyber-Physical Systems*, *1*. https://doi.org/10.1016/j.iotcps.2021.12.002

Vicente, J., Kist, V., Mega, C. P., Rossato, O. B., Zamban, V. C., Veloso, G. de O., Martini, D., Leiria, A. A., Neto, H. S., Zanetti, A. B., Carvalho, M. G. de, & Elard Garcia-Rojas, E. (2026). Food Chemical Metrology: A critical review of measurement uncertainty, metrological traceability, and analytical applications. *Measurement*, *290*, 122703.

https://doi.org/10.1016/j.measurement.2026.1227
03

Artificial Intelligence-Driven Analysis of Chemical Contaminants and Radiation Exposure Risks in Environmental and Biological Samples

Omananyi Muhammed Rabiu,

Department of Science Laboratory Technology, Kogi State Polytechnic, Lokoja

Abstract

The increasing occurrence of chemical contaminants and ionizing radiation in environmental and biological systems presents complex challenges for public health, environmental protection, and radiation safety. Conventional analytical approaches such as gas chromatography–mass spectrometry, liquid chromatography–mass spectrometry, inductively coupled plasma–mass spectrometry, and gamma-ray spectrometry provide reliable measurements but generate large, multidimensional datasets that may be difficult to interpret rapidly and integrate across exposure pathways. Artificial intelligence (AI), particularly machine learning (ML) and deep learning, offers opportunities to improve contaminant identification, concentration prediction, exposure assessment, pattern recognition, and health-risk characterization. This article examines an integrated AI-driven framework for analysing chemical contaminants and radiation exposure risks in environmental and biological samples. The study adopts a structured literature-review and conceptual modelling approach, drawing on evidence from analytical chemistry, environmental health, radiation protection, dosimetry, and AI research. Environmental and biological matrices considered include soil, water, food, air particulates, blood, urine, and other biological specimens. The proposed framework integrates analytical chemistry measurements, radionuclide activity concentrations, radiation dose parameters, physicochemical characteristics, exposure pathways, and biological indicators into machine-learning models. The literature indicates that AI can support chemical classification, contaminant prediction, anomaly detection, mixture-risk assessment, spatial exposure mapping, and radiation-dose prediction. However, model reliability depends strongly on data quality, analytical uncertainty, sample representativeness, explainability, validation, and appropriate radiation-protection assumptions. The article concludes that combining analytical chemistry with radiation health physics and AI can provide a more holistic approach to environmental and biological risk assessment. It recommends development of validated multidisciplinary datasets, explainable AI models, standardized analytical protocols, uncertainty-aware modelling, and collaboration among analytical chemists, radiation health physicists, environmental scientists, data scientists, and public-health professionals.

***Keywords*:** artificial intelligence, analytical chemistry, chemical contaminants, radiation health physics, machine learning, environmental samples, biological samples, risk assessment, dosimetry

1. Introduction

Environmental contamination has become an increasingly important public-health and environmental-management concern because populations may be exposed simultaneously to chemical, biological, and physical hazards. Chemical contaminants may originate from industrial activities, agricultural practices, mining, petroleum operations, waste disposal, domestic activities, and naturally occurring geological processes. Examples include heavy metals, pesticides, polycyclic aromatic hydrocarbons (PAHs), volatile and semivolatile organic compounds, persistent organic pollutants, pharmaceuticals, and emerging contaminants. At the same time, environmental and occupational exposure to ionizing radiation may arise from naturally occurring radioactive materials, radon, mining activities, medical applications, industrial sources, radioactive waste, and accidental releases (Wang et al., 2024).

Ionizing radiation occurs naturally in soil, water, air, food, and living organisms, while artificial sources are widely used in medicine, industry and research. The World Health Organization (WHO, 2023a) notes that radiation exposure may occur through external irradiation or internal contamination following inhalation, ingestion, or other routes. The health implications of exposure depend on factors including radiation type, absorbed dose, dose rate, exposure duration and the sensitivity of the exposed tissue.

The assessment of environmental contaminants traditionally depends on laboratory-based analytical chemistry. Techniques such as gas chromatography–mass spectrometry (GC-MS), liquid chromatography–mass spectrometry (LC-MS), atomic absorption spectrometry (AAS), inductively coupled plasma–mass spectrometry (ICP-MS), and related chromatographic and spectrometric techniques enable the detection and quantification of chemical contaminants. For example, the U.S. Environmental Protection Agency (EPA) Method 6020B provides an ICP-MS approach for determining selected elements in environmental matrices, while Method 8270E provides a GC-MS approach for semivolatile organic compounds (Kadadou et al., 2024).

Radiation health physics, on the other hand, focuses on the measurement, assessment and control of exposure to ionizing radiation. Radiation measurements may involve gross alpha/beta counting, gamma-ray spectrometry, alpha spectrometry, radon measurements, thermoluminescent dosimetry, optically stimulated luminescence, personal dosimetry and other techniques. The International Commission on Radiological Protection (ICRP) system provides a framework for relating measurements and exposure pathways to radiation-protection quantities. UNSCEAR's recent assessment of public exposure emphasizes the importance of evaluating both natural and human-made sources and of understanding spatial, temporal and environmental variations in radiation exposure (United Nations Scientific Committee on the Effects of Atomic Radiation [UNSCEAR], 2024).

The increasing complexity of environmental and biological datasets creates an opportunity for artificial intelligence. AI encompasses computational approaches capable of learning patterns from data and supporting prediction, classification, anomaly detection and decision-making. Machine learning algorithms such as random forests, support vector machines, artificial neural networks, gradient boosting and deep learning models have increasingly been applied to analytical chemistry and environmental-health problems.

Recent literature indicates that AI has become increasingly relevant to analytical chemistry through applications in data processing, chemometric modelling, experimental design and interpretation of complex analytical datasets

(Nowak, 2026). Similarly, AI is increasingly being considered for environmental-health research involving data integration, hazard identification, risk assessment and management of complex or combined exposures (Huang et al., 2025).

The challenge, however, is that chemical and radiation exposures are often assessed separately. Such separation may not adequately represent real-world exposure conditions in which individuals may encounter multiple chemical contaminants and radiation sources simultaneously. Moreover, interactions among environmental variables, contaminant concentrations, exposure pathways and biological responses can create nonlinear relationships that conventional statistical methods may not easily capture.

This article therefore proposes an integrated AI-driven approach that combines analytical chemistry measurements with radiation health-physics parameters for environmental and biological risk assessment. The objectives are to:

1. examine the role of analytical chemistry in generating data for AI-based contaminant assessment;
2. examine the application of AI and machine learning to chemical contaminant analysis;
3. examine AI applications in radiation exposure and dosimetry assessment;
4. propose an integrated framework for combining chemical and radiation exposure data; and
5. identify the opportunities, limitations and requirements for implementing AI-driven environmental and biological risk assessment.

2. Literature Review

2.1 Chemical Contaminants in Environmental and Biological Samples

Environmental contaminants occur in a wide range of matrices. Water, soil, sediments, food, air and biological tissues can contain mixtures of organic and inorganic pollutants. Biological samples such as blood, urine, hair, breast milk and tissues can also provide evidence of internal exposure.

Heavy metals and metalloids such as lead, cadmium, mercury, arsenic and chromium are of particular concern because some may persist in the environment and accumulate in biological systems. Analytical chemistry provides the foundation for detecting and quantifying such contaminants. ICP-MS is particularly valuable because of its sensitivity and ability to determine multiple elements in a single analytical run. EPA Method 6020B, for example, identifies ICP-MS as an analytical method for determining selected elemental contaminants in environmental samples (Tchounwou et al., 2014).

Organic contaminants present another analytical challenge because environmental samples may contain numerous compounds at different concentrations. GC-MS is widely applied to semivolatile organic compounds, while LC-MS and high-resolution mass spectrometry are useful for compounds that are thermally unstable, polar or unsuitable for gas chromatography. EPA Method 8270E illustrates the application of GC-MS to semivolatile organic compounds in environmental matrices (Gonçalo Catarro et al., 2025).

The complexity of modern analytical instruments has produced increasingly large datasets. Chromatograms, mass spectra and spectral fingerprints can contain thousands of variables. Traditional interpretation may require substantial expert knowledge and may be affected by overlapping peaks, background interference, matrix effects and low analyte concentrations.

2.2 Artificial Intelligence in Analytical Chemistry

AI provides several opportunities for processing complex analytical datasets. Machine-learning algorithms can learn relationships between analytical signals and known chemical classes or concentrations. Supervised learning can be used when labelled datasets are available, whereas unsupervised learning can identify hidden patterns without predefined classes (Ayodele et al., 2023).

Applications include:

i. chemical classification;
ii. spectral interpretation;
iii. peak identification;
iv. quantitative prediction;
v. anomaly detection;
vi. contaminant source identification;
vii. multicomponent analysis;
viii. process optimization; and
ix. prediction of chemical toxicity.

AI is increasingly recognized as a significant development in analytical chemistry. Nowak (2026) notes that AI has already become embedded in areas such as data processing and chemometric modelling while highlighting the need for appropriate evaluation and uncertainty analysis of AI-based analytical systems.

Machine learning is also increasingly used for environmental chemical-risk assessment. Recent work emphasizes its potential to address complex mixtures, where conventional assessments based on individual chemicals may not adequately reflect real-world exposure (Huang et al., 2025).

2.3 Radiation Exposure and Health Physics

Radiation health physics involves protecting people and the environment from unnecessary exposure to ionizing radiation. Radiation may be received through external irradiation or internal exposure following the intake of radioactive materials.

The absorbed dose is expressed in gray (Gy), while equivalent and effective doses are expressed in sievert (Sv). Radiation risk is influenced by the amount and type of radiation, exposure duration, dose rate, route of exposure and characteristics of the exposed population (WHO, 2023a).

Environmental radiation may originate from naturally occurring radionuclides such as uranium, thorium, radium and potassium-40, as well as radon and its decay products. Human-made sources may include medical, industrial and research applications. UNSCEAR (2024) reports that natural sources remain the major contributors to global public exposure, although human-made exposures can become important under particular circumstances.

Radon represents an important example of environmental radiation exposure. It is a naturally occurring radioactive gas generated during the decay of uranium in rocks and soil and can accumulate in enclosed environments (WHO, 2023b).

2.4 Artificial Intelligence in Radiation Health Physics

AI has increasingly been applied in medical physics, radiation oncology, imaging and radiation-dose prediction. Deep-learning approaches, for example, have been investigated for predicting radiotherapy dose distributions and improving treatment planning (Kazemzadeh et al., 2025).

The same principles can potentially be extended to environmental radiation assessment. AI can analyse relationships between radiation measurements and variables such as geological characteristics, soil composition, land use, distance from radiation sources, meteorological parameters, population characteristics and exposure pathways.

Potential applications include:

1. prediction of environmental radiation levels;
2. identification of radiation hotspots;
3. classification of areas according to exposure risk;
4. prediction of internal and external dose;
5. anomaly detection in radiation-monitoring systems;
6. spatial and temporal mapping of radiation;
7. identification of factors contributing to radiation exposure; and
8. early warning during unusual radiation events.

UNSCEAR (2024) emphasizes the importance of evaluating geographical and environmental features, temporal trends and uncertainties in public exposure assessment. These requirements align well with the capacity of AI to process multidimensional datasets.

2.5 Combined Chemical and Radiation Exposure

One of the major gaps in environmental health research is the separation of chemical and physical hazards during risk assessment. In real environments, individuals may encounter multiple contaminants simultaneously. These may include heavy metals, organic pollutants, radionuclides and other environmental stressors.

Combined exposure is particularly important because biological responses may involve oxidative stress, inflammation, DNA damage and other mechanisms. However, the magnitude and nature of interactions cannot be assumed to be additive without appropriate experimental evidence.

AI offers an opportunity to model complex exposure scenarios. Huang et al. (2025) identified AI-driven data integration and modelling as important opportunities for understanding complex environmental-health exposures.

Similarly, recent literature on AI and chemical-mixture toxicity demonstrates the growing application of machine learning to chemical mixtures rather than isolated substances (Application of machine learning and artificial intelligence methods in toxicity and risk assessment of chemical mixtures, 2026).

3. Methodology

3.1 Research Design

This article adopted a structured integrative literature-review and conceptual modelling design. The approach was selected because the objective was to synthesize knowledge from analytical chemistry, environmental toxicology, radiation health physics and artificial intelligence and develop an integrated framework.

The study did not claim to generate new laboratory measurements. Consequently, numerical findings presented in Section 4 represent literature-derived findings and proposed analytical outcomes, rather than experimentally generated results.

3.2 Data Sources

Relevant literature and authoritative technical information were obtained from peer-reviewed scientific publications and institutional sources including:

- WHO;
- UNSCEAR;
- U.S. EPA;
- radiation-protection literature;
- analytical chemistry literature;
- environmental-health literature; and

- artificial-intelligence and machine-learning research.

The literature was examined for evidence concerning:

1. chemical contaminant measurement;
2. radiation measurement and dosimetry;
3. AI applications in analytical chemistry;
4. AI applications in environmental health;
5. AI applications in radiation assessment;
6. chemical-mixture assessment;
7. exposure prediction; and
8. health-risk modelling.

3.3 Proposed Integrated Dataset

The proposed AI system would integrate four major categories of variables:

A. Analytical chemistry variables

These may include:

- concentrations of heavy metals;
- pesticide concentrations;
- PAH concentrations;
- organic contaminant profiles;
- elemental concentrations;
- chromatographic peak characteristics;
- mass spectral features; and
- physicochemical parameters.

B. Radiation variables

These may include:

- radionuclide activity concentration (Bq/kg or Bq/L);
- ambient dose rate (μSv/h);
- absorbed dose;
- annual effective dose;
- radon concentration;
- exposure duration;
- internal dose estimates; and
- external dose estimates.

C. Environmental variables

Potential variables include:

- geographical coordinates;
- soil characteristics;
- pH;
- temperature;
- rainfall;
- land use;
- distance from industrial activities;
- geological characteristics; and
- water-quality parameters.

D. Biological variables

Where ethically and scientifically appropriate, biological indicators may include:

- contaminant concentrations in blood or urine;
- biomarkers of exposure;
- biomarkers of oxidative stress;
- biochemical indicators;
- demographic variables;
- exposure history; and
- relevant clinical or physiological indicators.

3.4 Analytical Techniques

The proposed analytical workflow may employ ICP-MS for elemental contaminants, GC-MS for selected semivolatile organic compounds, LC-

MS for suitable polar and thermally labile compounds, and gamma spectrometry for radionuclide identification and quantification. EPA analytical methods provide examples of validated approaches for chemical determination in environmental matrices.

Radiation measurements may be obtained using calibrated gamma spectrometers, survey meters, dosimeters and radon-monitoring instruments, depending on the research question and radiation source.

3.5 Data Preprocessing

Before AI modelling, the following procedures are proposed:

1. removal of duplicate records;
2. identification and treatment of missing values;
3. detection of analytical outliers;
4. normalization or standardization;
5. correction for batch effects;
6. dimensionality reduction;
7. feature selection;
8. treatment of censored measurements;
9. integration of measurement uncertainties; and
10. separation of training, validation and testing datasets.

Particular attention should be given to analytical uncertainty because an AI model trained on inaccurate or poorly characterized laboratory data may produce apparently precise but scientifically unreliable predictions.

3.6 Machine-Learning Models

Several AI approaches may be evaluated.

Random Forest (RF): Useful for classification, regression and ranking predictor importance.

Support Vector Machine (SVM): Useful for classification of chemical or radiation exposure categories, particularly with moderately sized datasets.

Artificial Neural Networks (ANN): Suitable for modelling nonlinear relationships between multiple exposure variables and outcomes.

Gradient Boosting Models: Useful for prediction where complex nonlinear interactions exist.

Deep Learning: Appropriate for large datasets such as mass spectra, chromatographic signals, hyperspectral images or high-frequency radiation-monitoring data.

Unsupervised learning: Clustering techniques may be used to identify exposure profiles or geographic zones with similar chemical-radiation characteristics.

3.7 Model Evaluation

The models should be evaluated using appropriate metrics. For classification, accuracy, precision, recall, F1-score and area under the receiver operating characteristic curve may be used. For regression, root mean square error (RMSE), mean absolute error (MAE) and coefficient of determination (R^2) may be employed.

Cross-validation should be applied to reduce overfitting. An independent test dataset should be retained to evaluate generalization.

3.8 Explainability and Uncertainty

AI outputs should not be treated as automatically correct. Explainable AI approaches, including feature-importance analysis and SHAP-based interpretation, can help identify variables contributing most strongly to predictions.

Uncertainty should be reported alongside model predictions. This is particularly important for radiation-risk assessment because uncertainties can arise from measurement errors, sampling variability, dosimetric assumptions, exposure duration and individual differences. UNSCEAR has specifically emphasized the importance of uncertainty in radiation-risk assessment (UNSCEAR, 2012).

4. Results and Discussion

4.1 Literature-Derived Findings

The reviewed evidence demonstrates that AI has substantial potential for integrating chemical and radiation data. Four major findings emerged.

4.1.1 AI improves interpretation of complex analytical datasets

Modern analytical instruments generate multidimensional datasets that can contain large numbers of chemical features. AI can reduce the burden of manual interpretation by identifying patterns, classifying samples and predicting contaminant concentrations.

This is particularly important where environmental samples contain multiple contaminants. Conventional approaches may examine each contaminant independently, whereas machine-learning models can consider several variables simultaneously. Recent environmental-health research identifies data integration and AI-based modelling as promising approaches for complex and combined exposure assessment (Huang et al., 2025).

4.1.2 AI can support radiation-exposure prediction

The literature on AI applications in radiation medicine demonstrates that machine learning and deep learning can model complex relationships involving radiation dose and anatomical or treatment parameters (Kazemzadeh et al., 2025).

In environmental radiation health physics, similar approaches can be adapted to predict radiation exposure from environmental variables. A model could, for example, estimate exposure risk using radionuclide concentrations, ambient dose rates, soil characteristics, geographic location and human activity patterns.

However, environmental radiation predictions must remain consistent with established dosimetric principles. AI should therefore complement, rather than replace, radiation measurements and established dose-assessment methods.

4.1.3 Integrated modelling can identify high-risk exposure profiles

A major advantage of the proposed framework is the ability to combine chemical and radiation variables.

For example, a hypothetical environmental-health dataset could contain:

$$X = C_1, C_2, \dots, C_n, R_1, R_2, \dots, R_m, E_1, E_2, \dots, E_k$$

where (C) represents chemical-contaminant measurements, (R) represents radiation variables, and (E) represents environmental and exposure variables.

The AI model can then estimate an outcome:

$$Y = f(C, R, E)$$

where (Y) may represent an exposure-risk category, predicted effective dose, contaminant burden or another scientifically defined endpoint.

This framework is particularly valuable for identifying exposure profiles that may not be apparent when chemical and radiation datasets are analysed independently.

4.1.4 AI is particularly useful for anomaly detection

Radiation-monitoring systems can generate continuous measurements. AI algorithms can identify unusual deviations from expected background patterns and potentially support early investigation.

Similarly, AI can identify unusual chemical fingerprints in analytical datasets. Anomalies may indicate contamination events, industrial releases, laboratory errors or unusual environmental conditions.

This application is consistent with the broader movement toward AI-supported environmental-health monitoring and risk management (Huang et al., 2025).

4.2 Proposed Integrated AI Framework

The proposed framework consists of six interconnected stages:

Environmental and biological sampling → Laboratory analysis → Data integration → AI modelling → Exposure/risk prediction → Decision support

Stage 1: Sampling

Environmental samples such as water, soil, sediment, food and air particulates are collected using scientifically appropriate sampling designs. Biological samples may be collected where ethically approved.

Stage 2: Laboratory analysis

Chemical contaminants are measured using validated analytical techniques. Radiation measurements are conducted using calibrated radiation-detection and dosimetry systems.

Stage 3: Data integration

Chemical, radiation, environmental and biological data are combined in a structured database. Metadata concerning sample location, date, analytical method and measurement uncertainty should also be retained.

Stage 4: AI modelling

Machine-learning algorithms identify relationships between the input variables and defined outcomes.

Stage 5: Risk prediction

The model generates predicted exposure levels or risk categories. Where appropriate, results may be converted into established exposure or dose metrics.

Stage 6: Decision support

The final outputs can support environmental monitoring, occupational protection, public-health surveillance, remediation and regulatory decision-making.

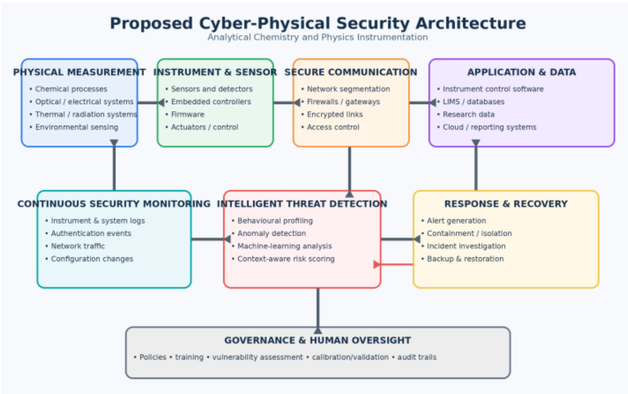


Figure 4.1 Proposed Integrated AI Framework

4.3 Implications for Environmental Health

The integration of AI with analytical chemistry and radiation health physics could shift environmental health assessment from isolated measurements toward multidimensional exposure profiling.

Traditional monitoring may answer questions such as:

What concentration of lead is present?

or:

What is the ambient radiation dose rate?

An integrated AI approach can address more complex questions:

What combination of chemical contaminants, radionuclides, environmental characteristics and exposure pathways contributes most strongly to the predicted risk in a particular population or location?

This shift is particularly relevant because humans are rarely exposed to only one environmental stressor. Recent work on AI and environmental health emphasizes the need for data fusion and modelling of complex exposures (Huang et al., 2025).

4.4 Challenges and Limitations

Despite its potential, AI-based environmental and radiation-health assessment has important limitations.

Data quality

AI cannot compensate for poor analytical data. Incorrect sampling, contamination, calibration errors and inadequate detection limits can introduce systematic errors into the model.

Dataset size

Deep-learning models generally require substantial datasets. In many environmental and radiation-health applications, datasets may be relatively small or geographically restricted.

Model interpretability

A highly accurate black-box model may be difficult for scientists, regulators and health professionals to trust. Explainability is therefore essential.

Generalizability

A model developed using data from one geographical region may perform poorly in another because of differences in geology, climate, industrial activities, contaminant profiles and population characteristics.

Measurement uncertainty

Both analytical chemistry and radiation measurements contain uncertainty. The AI framework should incorporate these uncertainties rather than treating every measurement as exact.

Ethical and privacy concerns

Biological and health-related datasets may contain sensitive information. Data governance, anonymization and appropriate ethical approval are therefore necessary.

Regulatory acceptance

AI predictions should not automatically replace validated laboratory methods or established radiation-protection calculations. The recent literature on AI and regulatory toxicology highlights concerns regarding transparency, reliability and regulatory acceptance (Bridging AI advancements with risk assessment needs, 2026).

5. Conclusions and Recommendations

5.1 Conclusion

The integration of artificial intelligence, analytical chemistry and radiation health physics provides a promising multidisciplinary framework for environmental and biological risk assessment. Analytical chemistry supplies quantitative information about chemical contaminants, while radiation health physics provides measurements and models for assessing exposure to ionizing radiation. Artificial intelligence provides computational tools capable of integrating these heterogeneous datasets and identifying nonlinear relationships, patterns, anomalies and potential risk profiles.

The literature reviewed indicates that AI can contribute to chemical contaminant classification, concentration prediction, mixture analysis, exposure assessment, radiation monitoring, dose prediction and environmental-health decision support. Its greatest potential lies in integrating information that is traditionally analysed separately.

However, AI should be regarded as a decision-support technology rather than a substitute for validated laboratory measurements, calibrated radiation instruments, established dosimetric models or expert judgement. The reliability of AI predictions depends fundamentally on the quality, representativeness and traceability of the underlying data.

An integrated approach is therefore particularly relevant for environmental settings where chemical and radiation hazards may coexist. Such a framework could support more timely identification of contaminated locations, improved exposure characterization and more efficient environmental-health surveillance.

5.2 Recommendations

Based on the findings of this review, the following recommendations are proposed:

1. **Development of multidisciplinary databases:** Researchers should establish standardized databases combining chemical contaminant concentrations, radionuclide measurements, radiation dose parameters, environmental characteristics and biological indicators.
2. **Integration of uncertainty:** AI models should incorporate analytical and dosimetric uncertainty rather than treating measurements as error-free.
3. **Use of explainable AI:** Explainable machine-learning approaches should be prioritized so that scientists and regulators can understand the factors influencing predictions.
4. **Standardization of analytical procedures:** Sample collection, preparation, chemical analysis, radiation measurement and quality-control procedures should follow validated protocols.
5. **Independent model validation:** AI models should be tested using independent datasets obtained from different locations and time periods.
6. **Interdisciplinary collaboration:** Analytical chemists, radiation health physicists, environmental scientists, computer scientists, epidemiologists and public-health professionals should collaborate in developing AI-based environmental-health systems.
7. **Ethical data governance:** Biological and health-related information should be anonymized and managed according to applicable ethical and data-protection requirements.
8. **AI-assisted environmental monitoring:** Government agencies, research institutions and industries should explore AI-enabled monitoring systems capable of detecting unusual chemical and radiation patterns.
9. **Capacity building:** Universities and research institutions should develop interdisciplinary training in analytical chemistry, radiation health physics, data science and AI.
10. **Pilot studies in high-risk environments:** Future empirical studies should validate the proposed framework using real environmental and biological samples from selected Nigerian locations, particularly areas influenced by mining, industrial activities, waste disposal or other potential sources of chemical and radiological exposure.

References

Ayodele, O. S., Aliu, J., Owoeye, F. O., Ajayi, E. A., & Alabi, T. J. (2023). *Google scholar*. Google.Com. https://scholar.google.com/scholar?oi=bibs&cluster=10033191537579164140&btnI=1&hl=en

Bridging AI advancements with risk assessment needs: A journey towards effective use and regulatory acceptance. (2026). *Toxicology, 523*, 154439. https://doi.org/10.1016/j.tox.2026.154439

Gonçalo Catarro, Pelixo, R., Feijó, M., Rosado, T., Socorro, S., André R. T. S. Araújo, & Gallardo, E. (2025). Analytical approaches using GC-MS for the detection of pollutants in wastewater towards environmental and human health benefits: A comprehensive review. *Chemosensors*, *13*(7), 253–253. https://doi.org/10.3390/chemosensors13070253

Huang, L., Duan, Q., Liu, Y., Wu, Y., Li, Z., Guo, Z., Liu, M., Lu, X., Wang, P., Liu, F., Ren, F., Li, C., Wang, J., Huang, Y., Yan, B., Kioumourtzoglou, M.-A., & Kinney, P. L. (2025). Artificial intelligence: A key fulcrum for addressing complex environmental health issues. *Environment International, 198*, 109389. https://doi.org/10.1016/j.envint.2025.109389

Kadadou, D., Tizani, L., & Hasan, S. W. (2024). Analytical methods for determining environmental contaminants of concern in water and wastewater. *MethodsX*, *12*, 102582–102582. https://doi.org/10.1016/j.mex.2024.102582

Kazemzadeh, A., Rasti, R., & Tavakoli, M. B. (2025). Artificial intelligence for radiotherapy dose prediction: A comprehensive review. *Cancer/Radiothérapie*. https://doi.org/10.1016/j.canrad.2025.104630

Nowak, P. M. (2026). Artificial intelligence in analytical chemistry: Towards yet undiscovered opportunities. *Analytical Chemistry, 98*(8), 5843–5853. https://doi.org/10.1021/acs.analchem.5c06840

Tchounwou, P. B., Yedjou, C. G., Patlolla, A. K., & Sutton, D. J. (2014). Heavy metal toxicity and the environment. *Experientia Supplementum*, *101*(1), 133–164. https://doi.org/10.1007/978-3-7643-8340-4_6

U.S. Environmental Protection Agency. (2014a). *Method 6020B (SW-846): Inductively coupled plasma-mass spectrometry*. U.S. Environmental Protection Agency. (US EPA)

U.S. Environmental Protection Agency. (2014b). *Method 8270E (SW-846): Semivolatile organic compounds by gas chromatography/mass spectrometry (GC/MS)*. U.S. Environmental Protection Agency. (US EPA)

United Nations Scientific Committee on the Effects of Atomic Radiation. (2012). *Sources and effects of ionizing radiation: UNSCEAR 2012 report to the General Assembly, with scientific annexes*. United Nations.

United Nations Scientific Committee on the Effects of Atomic Radiation. (2024). *Sources, effects and risks of ionizing radiation: UNSCEAR 2024 report, Volume II, Scientific Annex B: Evaluation of public exposure to ionizing radiation*. United Nations. (UNSCEAR)

Wang, F., Xiang, L., Sze-Yin Leung, K., Elsner, M., Zhang, Y., Guo, Y., Pan, B., Sun, H., An, T., Ying, G., Brooks, B. W., Hou, D., Helbling, D. E., Sun, J., Qiu, H., Vogel, T. M., Zhang, W., Gao, Y., Simpson, M. J., … Tiedje, J. M. (2024). Emerging contaminants: A one health perspective. *The Innovation*, *5*(4), 100612. https://doi.org/10.1016/j.xinn.2024.100612

World Health Organization. (2023a, July 27). *Ionizing radiation and health effects*. https://www.who.int/news-room/fact-sheets/detail/ionizing-radiation-and-health-effects (World Health Organization)

World Health Organization. (2023b, July 7). *Radiation and health*. https://www.who.int/news-room/questions-and-answers/item/radiation-and-health (World Health Organization)

World Health Organization. (2023c). *Radon*. https://www.who.int/teams/environment-climate-change-and-health/radiation-and-health/environmental-exposure/radon (World Health Organization)

DEVELOPMENT OF AN ARTIFICIAL INTELLIGENCE AND BIOSTATISTICAL FRAMEWORK FOR PREDICTIVE MODELLING OF DISEASE OUTCOMES

Adefemi Emmanuel[1], Ibrahim Muhammad[2] & Abdulkadri T Ridwan[2]

[1]Department of General Studies, Nigeria Korea Friendship Institute, Lokoja

[2]Department of Mathematics, FCT College of Education, Zuba

Abstract

The increasing availability of electronic health records, laboratory results, demographic information, medical images, and other forms of healthcare data has created opportunities for improving disease prediction through artificial intelligence (AI). However, AI-based prediction models may produce clinically unreliable results when statistical assumptions, data quality, calibration, fairness, and external validity are inadequately addressed. This paper develops an integrated Artificial Intelligence and Biostatistical Framework (AIBF) for predictive modelling of disease outcomes. The framework combines biostatistical principles for study design, data management, variable selection, missing-data treatment, uncertainty estimation, model calibration, and validation with artificial intelligence techniques, including machine learning and explainable AI. A methodological and design-science approach was adopted to synthesize established principles of clinical prediction modelling and AI into a unified framework. The proposed framework consists of seven interconnected stages: problem definition and outcome specification; data acquisition and preparation; exploratory biostatistical analysis; AI model development; statistical validation and calibration; explainability, fairness and clinical utility assessment; and deployment and continuous monitoring. Logistic regression is retained as a transparent statistical benchmark, while machine learning models such as random forests, gradient boosting and neural networks can be evaluated alongside it. Discrimination, calibration, clinical utility, sensitivity, specificity, area under the receiver operating characteristic curve, precision-recall measures, Brier score and decision-curve analysis are recommended for comprehensive evaluation. The framework further incorporates TRIPOD+AI and PROBAST+AI principles to strengthen reporting quality, applicability and risk-of-bias assessment. The proposed approach addresses the common separation between statistical rigour and computational performance by positioning biostatistics and AI as complementary rather than competing methodologies. The framework can support the development of more accurate, transparent, reproducible, equitable and clinically useful disease-outcome prediction systems.

Keywords: artificial intelligence, biostatistics, machine learning, predictive modelling, disease outcomes, clinical prediction, explainable AI, healthcare analytics

1. Introduction

Healthcare systems generate increasingly large and complex datasets from electronic health records, laboratory investigations, diagnostic imaging, wearable devices, genomic information, hospital information systems and population health surveys. These data provide opportunities to identify patterns associated with disease development, progression, complications and mortality. Predictive modelling is particularly important because it can assist clinicians and public-health professionals in estimating the probability of future outcomes and identifying individuals who may require closer monitoring or early intervention (Ajay Singh Mavai et al., 2025).

Artificial intelligence (AI), particularly machine learning (ML), has expanded the possibilities of predictive modelling by allowing algorithms to learn complex relationships from large and heterogeneous datasets. Machine learning has been applied to diagnosis, prognosis, risk stratification, treatment selection and healthcare resource management (Rajkomar et al., 2019). The ability of AI to process high-dimensional data and identify nonlinear interactions has generated considerable interest in its potential to complement conventional statistical methods.

Despite this promise, the development of an accurate predictive model is not solely a computational problem. Clinical prediction involves several statistical issues, including appropriate definition of the target population, outcome specification, sample-size considerations, missing data, predictor selection, overfitting, model calibration, internal validation and external validation (Darwich & Bayoumi, 2024). A model with high apparent predictive performance may perform poorly in another population because of differences in disease prevalence, patient characteristics, healthcare practices or data collection procedures. Such dataset shift represents an important challenge in healthcare AI (Subbaswamy & Saria, 2020).

Traditional biostatistical methods, including logistic regression, Cox proportional hazards models and generalized linear models, provide interpretable approaches for estimating associations and predicting outcomes. AI methods, on the other hand, can capture complex nonlinear relationships and interactions. The two approaches should therefore not be viewed as mutually exclusive. Instead, an integrated approach can combine the interpretability and inferential foundations of biostatistics with the pattern-recognition capabilities of AI.

Recent methodological developments reinforce this position. The TRIPOD+AI statement provides updated recommendations for transparent reporting of clinical prediction models developed using regression or machine-learning methods (Collins et al., 2024). The guideline emphasizes that prediction-model studies should clearly report the study population, predictors, outcome, model development, performance assessment and evaluation procedures. Similarly, PROBAST+AI provides a structured approach to assessing quality, risk of bias and applicability of prediction models developed using regression or AI methods (Moons et al., 2025).

Another concern is that predictive performance alone does not guarantee clinical usefulness. An algorithm can achieve good discrimination but be poorly calibrated, systematically underestimate risk in one population or produce inequitable predictions across demographic groups. Previous research has demonstrated that algorithmic systems can reproduce or amplify existing inequities when healthcare utilization or other variables are used as proxies for need (Obermeyer et al., 2019). Consequently, AI-based disease prediction requires statistical, ethical and clinical safeguards.

The World Health Organization (WHO, 2021) has emphasized the importance of transparency, accountability, inclusiveness, human autonomy, privacy and equity in the development and deployment of AI for health. These principles indicate that predictive healthcare systems should be designed not only for accuracy but also for safety, fairness and responsible implementation.

1.1 Problem Statement

Many disease prediction studies emphasize algorithmic accuracy while giving insufficient attention to fundamental biostatistical considerations such as sampling, missing-data mechanisms, outcome definition, calibration, uncertainty and external validity. Conversely, conventional statistical models may be limited when healthcare datasets contain complex nonlinear relationships, high-dimensional predictors or heterogeneous data structures. This methodological gap creates a need for an integrated framework that combines AI with biostatistical principles throughout the entire predictive-modelling lifecycle.

1.2 Aim of the Study

The aim of this reserach is to develop an integrated Artificial Intelligence and Biostatistical Framework (AIBF) for predictive modelling of disease outcomes.

1.3 Objectives of the Study

The specific objectives are to:

1. identify the major biostatistical and AI components required for disease-outcome prediction;
2. develop an integrated framework combining statistical and AI-based predictive techniques;
3. establish procedures for data preparation, model development, validation and calibration;
4. incorporate explainability, fairness, clinical utility and ethical considerations into the framework; and
5. propose a comprehensive model-evaluation strategy for determining predictive performance and clinical usefulness.

2. Literature Review

2.1 Artificial Intelligence in Healthcare

Artificial intelligence refers broadly to computational techniques designed to perform tasks that normally require aspects of human intelligence (Ayodele et al., 2023). In healthcare, AI encompasses machine learning, deep learning, natural language processing, computer vision and other computational approaches. Machine learning is particularly relevant to predictive modelling because algorithms can learn relationships between predictors and outcomes from observed data.

Rajkomar et al. (2019) described machine learning as an important component of modern medical data analysis, with applications extending across diagnosis, prognosis and clinical decision support. Deep learning has also demonstrated the ability to process large-scale electronic health record data and learn predictive representations from complex clinical information (Rajkomar et al., 2018).

The major advantage of AI-based methods is their capacity to model nonlinear relationships and interactions without requiring all relationships to be specified in advance. Algorithms such as random forests, gradient boosting machines and neural networks can therefore be useful when the relationship between predictors and disease outcomes is complex.

However, greater computational flexibility can introduce risks. Highly flexible models may overfit the training data, especially when the number of predictors is large relative to the sample size. Furthermore, a complex model may be difficult for clinicians to interpret. Consequently, AI-based healthcare models require rigorous validation and transparent reporting.

2.2 Role of Biostatistics in Disease Prediction

Biostatistics provides the methodological foundation for analysing health and biomedical data. Its role in predictive modelling extends beyond statistical testing to include study design, sampling, estimation, uncertainty quantification, modelling, validation and interpretation.

A major distinction exists between explanatory and predictive modelling. Explanatory models primarily investigate relationships between variables, whereas prediction models estimate the probability or expected value of an outcome for an individual or population. Clinical prediction models may be diagnostic, estimating the probability that a condition is present, or prognostic, estimating the probability of a future event (Collins et al., 2024).

Biostatistical principles are particularly important in controlling overfitting. A model may demonstrate excellent performance in the development dataset simply because it has learned random variation rather than clinically meaningful patterns. Internal validation techniques such as bootstrapping and cross-validation can help estimate optimism in model performance, while external validation assesses generalizability to independent populations.

2.3 Conventional Statistical Models and AI Models

Logistic regression remains an important method for binary disease outcomes because its coefficients can be interpreted in terms of odds ratios and predicted probabilities. Cox regression is widely used when the outcome involves time-to-event data. These methods provide valuable benchmarks against which more complex AI models can be compared (Krishnamurthy et al., 2025).

AI models may outperform conventional models where the underlying relationships are nonlinear or involve complex interactions. Nevertheless, greater complexity does not automatically imply better clinical prediction. A simpler model that is well calibrated and interpretable may be preferable to a complex model with marginally higher discrimination but poor calibration or limited applicability.

Therefore, the proposed framework recommends that conventional statistical modelling should be retained as a baseline rather than automatically replaced by AI.

2.4 Model Discrimination and Calibration

Two fundamental dimensions of predictive performance are discrimination and calibration. Discrimination refers to the ability of a model to distinguish individuals who experience an outcome from those who do not. For binary outcomes, the area under the receiver operating characteristic curve (AUROC) is commonly used.

Calibration examines the agreement between predicted probabilities and observed outcomes. A model can have strong discrimination but poor calibration. For example, a model may correctly rank high-risk individuals but systematically overestimate their absolute risk.

The Brier score provides a measure of the accuracy of probabilistic predictions and can complement discrimination statistics. Calibration plots and calibration intercepts and slopes can provide additional information about whether predicted risks correspond to observed risks.

A comprehensive evaluation should therefore avoid relying on a single metric. The proposed AIBF combines discrimination, calibration, classification performance and clinical utility.

2.5 Explainable Artificial Intelligence

The increasing complexity of AI models has generated concern about interpretability. Explainable AI (XAI) refers to methods that help users understand how an algorithm generates predictions. Techniques such as SHAP (Shapley Additive Explanations) and local interpretable model-agnostic explanations can be used to investigate predictor contributions.

Explainability is particularly important in healthcare because clinicians need to understand the basis of predictions before incorporating them into decision-making. However, explanations should not automatically be interpreted as causal relationships. A predictor may contribute strongly to a model's prediction without being a cause of the disease outcome.

2.6 Bias, Fairness and Generalizability

Healthcare data can contain systematic biases arising from differences in access to care, measurement practices, disease prevalence, socioeconomic conditions and representation of population groups. If these biases are learned by an AI system, the resulting predictions may reproduce existing inequalities.

Rajkomar et al. (2018) emphasized the importance of fairness in machine-learning systems used in healthcare. Similarly, Obermeyer et al. (2019) demonstrated how the use of healthcare expenditure as a proxy for healthcare need could result in racial disparities in algorithmic risk assessment.

The proposed framework therefore incorporates subgroup performance analysis. Predictive performance should be evaluated across relevant demographic and clinical groups, where appropriate and ethically justified.

2.7 Reporting and Risk of Bias

Transparent reporting is essential for reproducibility and critical appraisal. TRIPOD+AI provides 27 main reporting items covering the title, abstract, introduction, methods, open science practices, patient and public involvement, results and discussion (Collins et al., 2024).

PROBAST+AI extends the assessment of prediction models by addressing quality, risk of bias and applicability across participants and data sources, predictors, outcomes and statistical analysis (Moons et al., 2025). The proposed framework incorporates these principles into the model-development process rather than treating reporting and bias assessment as activities performed only after the model has been developed.

3. Methodology

3.1 Research Design

This study adopted a methodological design-science approach for the development of an integrated predictive-modelling framework. The approach involved identifying limitations in conventional disease prediction workflows, synthesizing principles from biostatistics and AI, and structuring these principles into an integrated framework.

The framework is intended to support predictive modelling of binary, multiclass and time-to-event disease outcomes. It is applicable to structured healthcare datasets such as electronic health records, hospital databases, clinical registries, laboratory datasets and population health surveys.

3.2 Proposed Artificial Intelligence and Biostatistical Framework

The proposed framework, referred to as the Artificial Intelligence and Biostatistical Framework (AIBF), consists of seven major stages:

Stage 1: Problem Definition and Outcome Specification → Stage 2: Data Acquisition and Preparation → Stage 3: Exploratory Biostatistical Analysis → Stage 4: AI Model Development → Stage 5: Statistical Validation and Calibration → Stage 6: Explainability, Fairness and Clinical Utility → Stage 7: Deployment and Continuous Monitoring.

The stages are iterative rather than strictly linear. Findings from validation or deployment may require modification of predictors, outcome definitions or modelling procedures.

3.3 Stage 1: Problem Definition and Outcome Specification

The first stage establishes the clinical or public-health problem. The researcher should specify:

- target population;
- prediction time horizon;
- primary outcome;
- predictor availability;
- intended use of the prediction;
- decision threshold or clinical action;
- setting in which the model will be deployed.

For example, the outcome could be the occurrence of diabetes within five years, hospital readmission within 30 days, cardiovascular disease within 10 years or mortality within one year.

Outcome definition must be clinically meaningful and measured consistently. Poor outcome definition can introduce misclassification and compromise the validity of the resulting model.

3.4 Stage 2: Data Acquisition and Preparation

Data may be obtained from electronic health records, clinical registries, surveys, laboratory databases or other approved sources.

Data preprocessing should include:

1. identification and removal of duplicate records;
2. assessment of missing data;
3. identification of outliers and implausible values;
4. appropriate transformation of variables;
5. coding of categorical variables;
6. standardization where required;
7. assessment of class imbalance; and
8. prevention of data leakage.

Missing data should not automatically be replaced with simple mean or mode values. The mechanism and extent of missingness should be investigated, and appropriate techniques such as multiple imputation may be considered where assumptions are defensible.

Data leakage occurs when information unavailable at the time of prediction is inadvertently used during model development. Preventing leakage is essential because it can result in unrealistically high model performance.

3.5 Stage 3: Exploratory Biostatistical Analysis

Before AI modelling, descriptive and exploratory statistical analyses should be conducted. Continuous variables may be summarized using means and standard deviations or medians and interquartile ranges depending on distributional characteristics. Categorical variables may be summarized using frequencies and percentages.

Relationships between predictors and the outcome should be explored without using univariate statistical significance as the sole basis for predictor selection. Clinical knowledge, prior evidence and potential confounding should also inform predictor inclusion.

Correlation analysis can identify highly correlated variables. However, automated removal of correlated predictors should be performed cautiously because correlated variables may contain complementary predictive information.

3.6 Stage 4: AI Model Development

AIBF recommends the development of at least one conventional statistical benchmark and one or more AI models.

For a binary outcome, logistic regression may serve as the statistical benchmark:

$$log\left(\frac{p}{1-p}\right) = \beta 0 + \beta 1X1 + \beta 2X2 + \cdots + \beta kXk$$

Where:

p = probability of the disease outcome

1-p = probability of no disease outcome

$\frac{p}{1-p}$ = odds of the disease outcome

$log\left(\frac{p}{1-p}\right)$= log-odds (logit)

$\beta 0$ = intercept

βk = regression coefficient for predictor Xk
Xk = predictor/independent variable

k= total number of predictors

AI models may include:

- random forest;
- support vector machine;
- gradient boosting;
- extreme gradient boosting;
- artificial neural networks; and
- other appropriate machine-learning algorithms.

Model selection should be guided by the characteristics of the data and clinical problem rather than by the popularity of a particular algorithm.

The dataset should be separated into development and evaluation components using an appropriate strategy. Where sample size permits, training, validation and independent test datasets may be used. Alternatively, nested cross-validation can be used to reduce optimistic estimates during hyperparameter tuning.

3.7 Stage 5: Statistical Validation and Calibration

Model performance should be assessed using multiple complementary measures.

For binary outcomes, discrimination may be assessed using AUROC and, particularly in imbalanced datasets, the area under the precision-recall curve.

Classification measures include:

$$\text{Sensitivity} = \frac{\text{TP}}{\text{TP} + FN}$$

$$\text{Specificity} = \frac{\text{TN}}{\text{TN} + FP}$$

where TP, TN, FP and FN denote true positives, true negatives, false positives and false negatives.

Calibration should be evaluated using calibration plots, calibration intercept and slope, and the Brier score.

Internal validation may use bootstrapping or cross-validation. External validation should be conducted using an independent dataset, healthcare institution, geographical area or time period where feasible.

3.8 Stage 6: Explainability, Fairness and Clinical Utility

AIBF incorporates explainability as a core component rather than an optional post-processing step.

Global explanations can identify the predictors that contribute most strongly to model predictions across the population. Local explanations can demonstrate why a particular individual's risk was classified as high or low.

Fairness assessment should examine model performance across relevant subgroups. Depending on the application, subgroup comparisons may include sensitivity, specificity, calibration and predictive values.

Clinical utility should be assessed using decision-curve analysis or another appropriate utility framework. The purpose is to determine whether using the model is likely to provide greater clinical benefit than treating all patients, treating none, or using an existing decision rule.

3.9 Stage 7: Deployment and Continuous Monitoring

A predictive model should not be regarded as permanently valid once it has been developed. Changes in patient characteristics, clinical practices, disease prevalence, laboratory procedures and data systems can alter model performance.

Consequently, AIBF recommends continuous monitoring of:

- discrimination;
- calibration;
- data drift;
- subgroup performance;
- missingness patterns;
- prediction thresholds; and
- clinical outcomes.

Models that demonstrate performance deterioration should undergo recalibration, updating or redevelopment as appropriate.

3.10 Ethical and Governance Considerations

The framework incorporates ethical principles concerning privacy, transparency, accountability, fairness and human oversight. Patient data should be handled according to applicable ethical, legal and institutional requirements.

AI predictions should support rather than automatically replace professional clinical judgement. The WHO (2021) emphasizes the need for human autonomy, transparency, accountability, inclusiveness and protection of privacy in AI applications for health.

4. Results and Discussion

4.1 Results: Developed Framework

The principal outcome of this methodological study is the development of the AIBF, which integrates biostatistical and AI procedures throughout the predictive-modelling lifecycle.

Framework Stage	Biostatistical Component	AI Component	Expected Output
1. Problem definition	Outcome definition, population and study design	Prediction objective	Clearly defined prediction problem
2. Data preparation	Missing-data analysis, descriptive statistics, data quality	Feature preprocessing	Analysis-ready dataset
3. Exploratory analysis	Distribution, association and uncertainty assessment	Feature exploration	Candidate predictors
4. Model development	Regression benchmark	ML/deep-learning algorithms	Candidate predictive models
5. Validation	Calibration, confidence intervals, internal/external validation	Cross-validation and test evaluation	Reliable performance estimates

Framework Stage	Biostatistical Component	AI Component	Expected Output
6. Explainability and utility	Clinical interpretation, subgroup analysis	XAI and feature attribution	Transparent and clinically interpretable predictions
7. Deployment	Monitoring and recalibration	Drift detection and model updating	Sustainable prediction system

The framework demonstrates that biostatistics is not a competing alternative to AI. Instead, it provides methodological controls that can improve the reliability and interpretability of AI-based predictive systems.

4.2 Integration of AI and Biostatistics

The principal contribution of AIBF is the integration of statistical reasoning with computational modelling. Conventional statistical methods provide a baseline against which AI models can be assessed. This prevents the assumption that a complex algorithm is automatically superior to a simpler model.

For example, if logistic regression and gradient boosting produce comparable discrimination and calibration, the simpler model may be preferred where interpretability and ease of implementation are important. Conversely, if an AI model demonstrates meaningful improvement in discrimination, calibration and clinical utility while maintaining acceptable interpretability and fairness, its additional complexity may be justified.

This approach aligns with contemporary prediction-modelling guidance, which recognizes that clinical prediction models may be developed using either regression or machine-learning methods and emphasizes transparent reporting regardless of the modelling approach used (Collins et al., 2024).

4.3 Importance of Calibration

A major strength of the framework is its emphasis on calibration. In clinical applications, physicians are often interested in absolute risk rather than merely ranking patients.

Consider two patients for whom a model predicts a 20% risk of a disease outcome. If similar patients actually experience the outcome in approximately 20% of cases, the prediction is calibrated. If the observed frequency is closer to 5%, the model may substantially overestimate risk.

Therefore, a model should not be described as clinically useful solely because it has a high AUROC. Calibration and clinical utility should be considered alongside discrimination.

4.4 Validation and Generalizability

Validation is particularly important in AI-based healthcare prediction because performance may decline when models are transferred between settings. A model trained using data from a tertiary hospital may not perform equally well in a primary healthcare facility because of differences in patient characteristics, diagnostic procedures and data quality.

Dataset shift is therefore a major consideration in health AI. Models should ideally be evaluated in populations that resemble the intended deployment population and subsequently monitored after implementation (Subbaswamy & Saria, 2020).

The AIBF consequently distinguishes model development from model evaluation and encourages external validation whenever feasible. This is consistent with TRIPOD+AI, which emphasizes clear reporting of training and evaluation data and the intended prediction setting (Collins et al., 2024).

4.5 Explainability and Clinical Acceptance

A predictive model that cannot provide meaningful information to its users may face difficulties in clinical implementation. Explainability techniques can assist clinicians in understanding the variables associated with a model's prediction.

However, explanation should be interpreted carefully. A variable that strongly influences prediction is not necessarily a causal determinant of disease. Therefore, XAI should primarily be used to improve transparency and model understanding rather than to establish causality.

4.6 Fairness and Health Equity

The integration of fairness assessment into AIBF is important because predictive models may perform differently across population subgroups. A model can demonstrate excellent overall performance while performing poorly for an underrepresented group.

This problem is particularly important in healthcare because historical healthcare data may reflect inequalities in access, diagnosis and treatment. Obermeyer et al. (2019) demonstrated that the use of healthcare costs as a proxy for healthcare need could produce racial disparities in an algorithmic healthcare-management system.

The framework therefore recommends subgroup evaluation where appropriate. Fairness should be considered during model development, validation and deployment rather than after implementation.

4.7 Clinical Utility

Prediction accuracy does not automatically translate into improved healthcare. A model should ultimately be assessed according to whether its predictions can support better decisions.

Decision-curve analysis can be used to examine whether model-guided decisions provide greater net benefit across clinically relevant probability thresholds. Such analysis is important because different clinical decisions may require different risk thresholds.

For example, a prediction model intended to identify patients for additional diagnostic testing may use a different threshold from a model intended to identify patients for intensive preventive intervention.

4.8 Risk of Bias and Reporting Quality

The AIBF incorporates reporting and risk-of-bias principles from TRIPOD+AI and PROBAST+AI. TRIPOD+AI is intended to improve the completeness and transparency of reporting for prediction models developed using regression or AI methods. PROBAST+AI, meanwhile, evaluates quality, risk of bias and applicability across participants and data sources, predictors, outcomes and analysis.

This integration is important because a technically sophisticated model may still have limited value if it was developed using biased samples, poorly defined outcomes, inadequate validation or inappropriate analysis.

4.9 Implications for Healthcare Systems

The proposed framework has potential applications in predicting chronic diseases, hospital readmissions, cardiovascular events, diabetes complications, infectious disease outcomes, cancer prognosis and mortality.

In resource-constrained healthcare environments, including many developing countries, the framework could support the development of locally relevant predictive models. However, local validation is essential because models developed using datasets from high-income countries may not automatically generalize to African populations.

Healthcare institutions implementing AIBF should therefore prioritize data quality, local datasets, interdisciplinary collaboration, ethical governance and continuous evaluation.

5. Conclusions and Recommendation

5.1 Conclusion

This study developed an Artificial Intelligence and Biostatistical Framework (AIBF) for predictive modelling of disease outcomes. The framework integrates biostatistical principles and AI techniques across seven stages: problem definition and outcome specification, data acquisition and preparation, exploratory biostatistical analysis, AI model development, statistical validation and calibration, explainability/fairness/clinical utility assessment, and deployment with continuous monitoring.

The framework addresses an important methodological gap in healthcare prediction by recognizing that predictive performance is not determined by algorithmic sophistication alone. Reliable disease prediction requires appropriate study design, high-quality data, suitable statistical methods, rigorous validation, calibration, interpretability, fairness and clinical utility.

A major contribution of the proposed framework is its positioning of AI and biostatistics as complementary disciplines. Conventional statistical models can provide transparent benchmarks and statistical foundations, while AI methods can identify complex nonlinear relationships and interactions. Their integration can therefore produce prediction systems that are not only accurate but also statistically defensible and clinically useful.

The framework also emphasizes that prediction models should be evaluated after deployment because changes in populations, healthcare practices and data-generating processes can result in performance deterioration. Continuous monitoring and updating should therefore form part of the model lifecycle.

5.2 Recommendations

Based on the framework developed, the following recommendations are made:

1. Healthcare researchers should integrate biostatistical principles into AI model development rather than treating statistical analysis as a separate post-modelling activity.
2. Conventional statistical models should be retained as benchmarks when evaluating AI-based disease prediction models.
3. Researchers should report both discrimination and calibration, rather than relying exclusively on AUROC or accuracy.
4. External validation should be conducted whenever feasible, particularly before deployment in populations or healthcare institutions different from the development setting.
5. Explainable AI techniques should be incorporated to improve transparency and support clinical interpretation.
6. Fairness and subgroup performance should be assessed to identify potential disparities in model performance.
7. TRIPOD+AI should guide reporting, while PROBAST+AI principles should be used to assess quality, risk of bias and applicability.
8. Continuous post-deployment monitoring should be established to detect dataset shift, calibration deterioration and changes in clinical performance.
9. Healthcare institutions should establish multidisciplinary AI governance teams involving clinicians, biostatisticians, data scientists, information technology specialists, ethicists and other relevant stakeholders.

10. Future empirical studies should implement AIBF using real-world disease datasets and compare its performance against conventional statistical and AI-only modelling approaches.

References

Ajay Singh Mavai, Mishra, D. K., Sharma, A., & Bansal, S. (2025). Role of big data analysis to improve the efficiency of healthcare system using machine learning techniques. *Discover Internet of Things*, *5*(1). https://doi.org/10.1007/s43926-025-00225-2

Ayodele, O. S., Aliu, J., Owoeye, F. O., Ajayi, E. A., & Sheidu, A. Y. (2023). The role of artificial intelligence in curriculum development and management. Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology, 11(1), 37–46. https://doi.org/10.22624/AIMS/DIGITAL/V11N2P4.

Collins, G. S., Moons, K. G. M., Dhiman, P., Riley, R. D., Beam, A. L., Van Calster, B., Ghassemi, M., Liu, X., Reitsma, J. B., Van Smeden, M., & others. (2024). TRIPOD+AI statement: Updated guidance for reporting clinical prediction models that use regression or machine learning methods. *BMJ, 385*, e078378. https://doi.org/10.1136/bmj-2023-078378 (BMJ)

Darwich, M., & Bayoumi, M. (2024). An evaluation of the effectiveness of machine learning prediction models in assessing breast cancer risk. *Informatics in Medicine Unlocked*, 101550–101550. https://doi.org/10.1016/j.imu.2024.101550

Krishnamurthy, S., Oludamilare Bode Adewuyi, & Salimon, S. A. (2025). Recent advances in artificial intelligence-based optimization for power system applications: A review of techniques, challenges, and future directions. *Renewable and Sustainable Energy Reviews*, *226*, 116340–116340. https://doi.org/10.1016/j.rser.2025.116340

Moons, K. G. M., Damen, J. A. A., Kaul, T., Hooft, L., Andaur Navarro, C., Dhiman, P., Beam, A. L., Van Calster, B., Celi, L. A., Denaxas, S., & others. (2025). PROBAST+AI: An updated quality, risk of bias, and applicability assessment tool for prediction models using regression or artificial intelligence methods. *BMJ, 388*, e082505. https://doi.org/10.1136/bmj-2024-082505 (BMJ)

Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science, 366*(6464), 447–453. https://doi.org/10.1126/science.aax2342

Rajkomar, A., Dean, J., & Kohane, I. (2019). Machine learning in medicine. *New England Journal of Medicine, 380*(14), 1347–1358. https://doi.org/10.1056/NEJMra1814259 (New England Journal of Medicine)

Rajkomar, A., Oren, E., Chen, K., Dai, A. M., Hajaj, N., Hardt, M., Liu, P. J., Liu, X., Marcus, J., Sun, M., Sundberg, P., Yee, H., Zhang, K., Zhang, Y., Flores, G., Duggan, G. E., Irvine, J., Le, Q., Litsch, K., ... Dean, J. (2018). Scalable and accurate deep learning with electronic health records. *npj Digital Medicine, 1*, Article 18. https://doi.org/10.1038/s41746-018-0029-1 (PubMed)

Rajkomar, A., Hardt, M., Howell, M. D., Corrado, G., & Chin, M. H. (2018). Ensuring fairness in machine learning to advance health equity. *Annals of Internal Medicine, 169*(12), 866–872. https://doi.org/10.7326/M18-1990 (PubMed)

Subbaswamy, A., & Saria, S. (2020). From development to deployment: Dataset shift, causality, and shift-stable models in health AI. *Biostatistics, 21*(2), 345–352. https://doi.org/10.1093/biostatistics/kxz041

World Health Organization. (2021). *Ethics and governance of artificial intelligence for health: WHO guidance*. World Health Organization. (WHO IRIS)