AJSTME, Volume. 12, Issue 2. 371-387, March, 2026. https://www.ajstme.com.ng
ISSN: 2251-0141 (Print), 2971-6233 (Online)

Computerized Record Processing Systems: A Review of Methodologies, Strategic Frameworks and Institutional Adoption

Tose E. Oziegbe[1], Veronica I. Osubor[2] & Emekumeh O. Sanctus[3]
[1]Department of Computer Science, Delta State University Abraka, Nigeria.
[2]Department of Computer Science, University of Benin, Nigeria
[3]Department of Computer Science, Southern Delta University, Ozoro, Delta State, Nigeria
Corresponding Authors: toseoziegbe@gmail.com

Abstract

This paper presents a systematic review of computerized record processing systems (CRPS). It synthesizes literature on methodologies, strategic frameworks, and institutional adoption patterns that characterize the shift from paper-based to electronic record processing systems (ERPS), in academic and institutional settings. Peer-reviewed studies published between 2018 and 2026 were reviewed covering: database management approaches, web- and cloud-based architectures, blockchain-based record systems, artificial intelligence and machine learning applications, application programming interface (API)-driven by interoperability frameworks, and mobile self-service portals. The review further examines the security frameworks that protect these systems including: role-based access control (RBAC), encryption, digital signatures and public-key infrastructure, and distributed-ledger approaches. The review concludes that computerized record processing systems deliver measurable gains in: speed, accuracy, and administrative efficiency. Nevertheless, methodological rigour, in particular a move beyond descriptive survey designs toward theoretically grounded and comparative research; is needed to build a robust evidence base for future institutional adoption.

Keywords: Computerized Record Processing Systems (CRPS), Electronic Record Processing Systems (ERPS), Data Encryption, Digital Signatures, Database Management Systems, Institutional Adoption.

Introduction

Institutions of every kind: universities, government registries, hospitals, banks, and courts; have historically depended on paper files and ledgers. As the volume, complexity and geographic spread of institutional activity has grown; manual approach has become increasingly difficult to sustain (Tose et al., 2026). Paper records are slow to retrieve, easily damaged or lost, costly to duplicate and vulnerable to unauthorized alteration that leaves no audit trail. These limitations have driven a decades-long, still ongoing transition toward computerized (or electronic) record processing systems (CRPS/ERPS). These systems capture, store, verify, and distributes records through integrated software and hardware infrastructure rather than paper (Tose et al., 2026).

This transition has evolved from early standalone database applications, through networked and later cloud-hosted platforms, to today's cryptographically anchored and artificial intelligence assisted systems. Nevertheless, new dependencies requiring funding for licensing and infrastructure, stable electricity and internet connectivity, and trained staffs have been introduced. Also, regulatory frameworks governing how personal and institutional data is collected, stored and shared are critical needs. In many parts of the world, and particularly across Sub-Saharan Africa, the adoption of computerized record processing systems has proceeded unevenly. Institutions frequently operate hybrid manual-electronic systems, part records still exist only on paper, while others have been digitized. The pace of full transition is shaped as much by infrastructural and human factors, as by the technology itself. This review is motivated by the need to consolidate what is known about the methodologies, strategic frameworks, and institutional adoption patterns that determine whether and how CRPS deployments succeed, so that future implementations are designed with a clearer view of the barriers and enablers documented in prior research.

Research Objectives

This study is guided by the following research objectives, to:

i. Systematically identify, evaluate, and synthesize peer-reviewed research on the methodologies, technologies, and architectures used in computerized record processing systems.
ii. Examine the security frameworks, compliance standards, and measures of regulation that govern the confidentiality, integrity, and availability of computerized records in a critical manner.
iii. Synthesize empirical literature on institutional adoption of computerized record processing systems, with much attention on the theoretical or conceptual frameworks used, the research designs adopted, factors for adoption and the barriers reported.
iv. Identify the methodological and practical limitations of existing computerized record processing systems, their strategic frameworks, and institutional adoption studies, and propose directions for future research.

Scope of the Study

This review focuses on computerized record processing (CRPS) systems deployed for institutional records: encompassing academic transcripts and certificates, administrative and personnel records, and comparable institutional documents. It covers the techniques and technologies used to build such systems: relational and NoSQL database management, cloud and web architectures, blockchain and distributed ledger technology, artificial intelligence and machine learning applications, API-driven interoperability, and mobile self-service portals; together with the security frameworks and compliance regimes that protect them. The review also covers empirical studies of institutional adoption, with particular attention to the theoretical frameworks, research designs, and adoption barriers reported across different institutional and national contexts.

Research Methodology

This systematic literature review was conducted following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework. IEEE Xplore, Scopus, Web of Science, ACM Digital Library, and Google Scholar were among the electronic databases searched using boolean search strings that combined terms such as ('computerized record' OR 'electronic record' OR 'digital record processing') AND ('database' OR 'cloud' OR 'blockchain' OR 'artificial intelligence' OR 'API' OR 'interoperability') for the technology strand, and ('institutional adoption' OR 'records management' OR 'ERPS' OR 'ERMS') AND ('university' OR 'tertiary institution' OR 'registrar' OR 'transcript') for the adoption strand.

Studies were included if they: (i) clearly addressed computerized or electronic record processing within an institutional context; (ii) reported a research methodology or system design that could be evaluated; (iii) provided sufficient detail on the framework, model, or system type used for summary or comparison; and (iv) were mostly published in peer-reviewed journals or conference proceedings between 2018 and 2026. Studies that addressed record processing purely as a general information technology topic, without any institutional or records management framing, or that did not report a research design, were excluded.

AJSTME, Volume. 12, Issue 2. 371-387, March, 2026. https://www.ajstme.com.ng
ISSN: 2251-0141 (Print), 2971-6233 (Online)

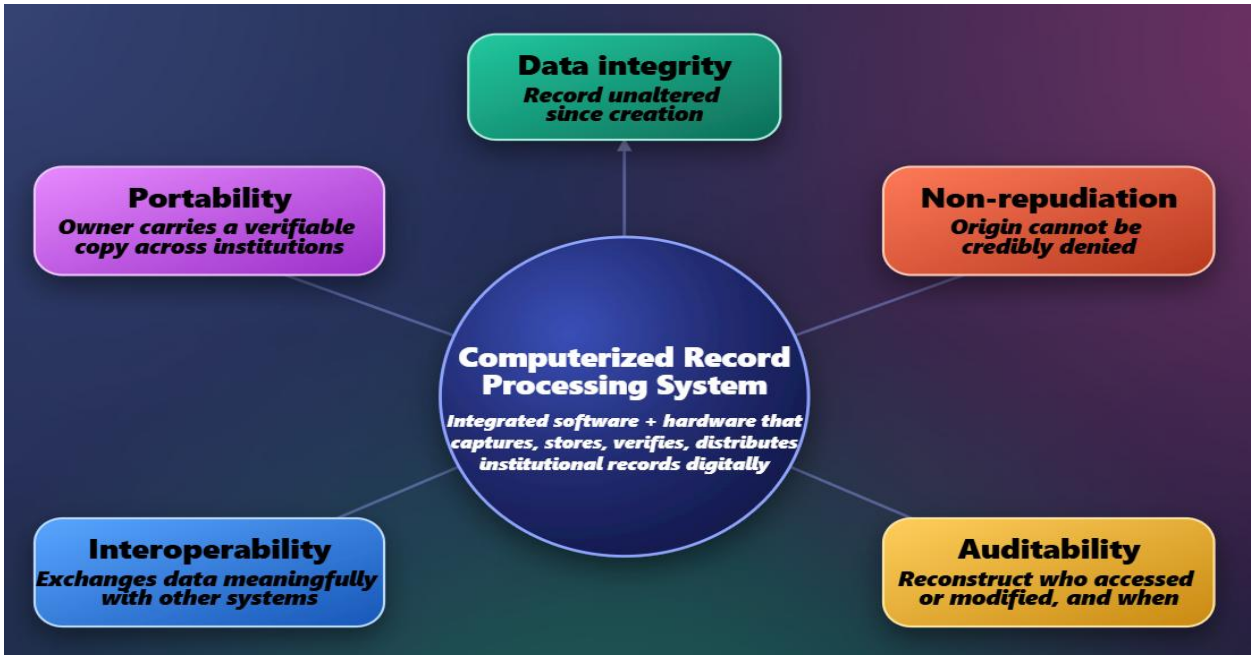

Figure 1: Concepts of computerized record processing systems

Overview of Computerized Record Processing Systems

Definition and Core Concepts

A computerized (or electronic) record processing system (CRPS) is an integrated software and hardware infrastructure that captures, stores, verifies, and distributes institutional records in digital form, replacing or supplementing paper-based equivalents (Ologbosere et al., 2025). Core concepts underpinning ERPS design include data integrity (assurance that a record has not been altered since creation), non-repudiation (assurance that a record's origin cannot be credibly denied), auditability (the ability to reconstruct who accessed or modified a record and when), interoperability (the ability of the system to exchange data meaningfully with other institutional or external systems), and increasingly portability (the ability of a student or graduate to carry a verifiable copy of their own record between systems and institutions without depending on continued access to the issuing institution's own infrastructure), Luyombya et al., (2020).

Evolution from Manual to Digital Transcript Systems

The evolution of transcript systems is traced roughly through five generations: (1) standalone, single-institution database applications with no external connectivity; (2) networked student information systems accessible over institutional intranets (Dano et al., 2021); (3) cloud-hosted, web- and mobile-accessible platforms supporting self-service requests and third-party verification portals; (4) cryptographically anchored systems, in which a hash or digital signature of a record is committed to a blockchain or similar tamper-evident ledger, and checking of authenticity is not dependent on the issuing institution's continued cooperation; and (5) an emerging generation of decentralized identity systems, in which the student or graduate holds a portable, cryptographically verifiable credential in a personal digital wallet; rather than relying on either the institution's database or a third-party verification portal at the point of use (Ibeneme-Sabinus et at., 2020).

AJSTME, Volume. 12, Issue 2. 371-387, March, 2026. https://www.ajstme.com.ng
ISSN: 2251-0141 (Print), 2971-6233 (Online)

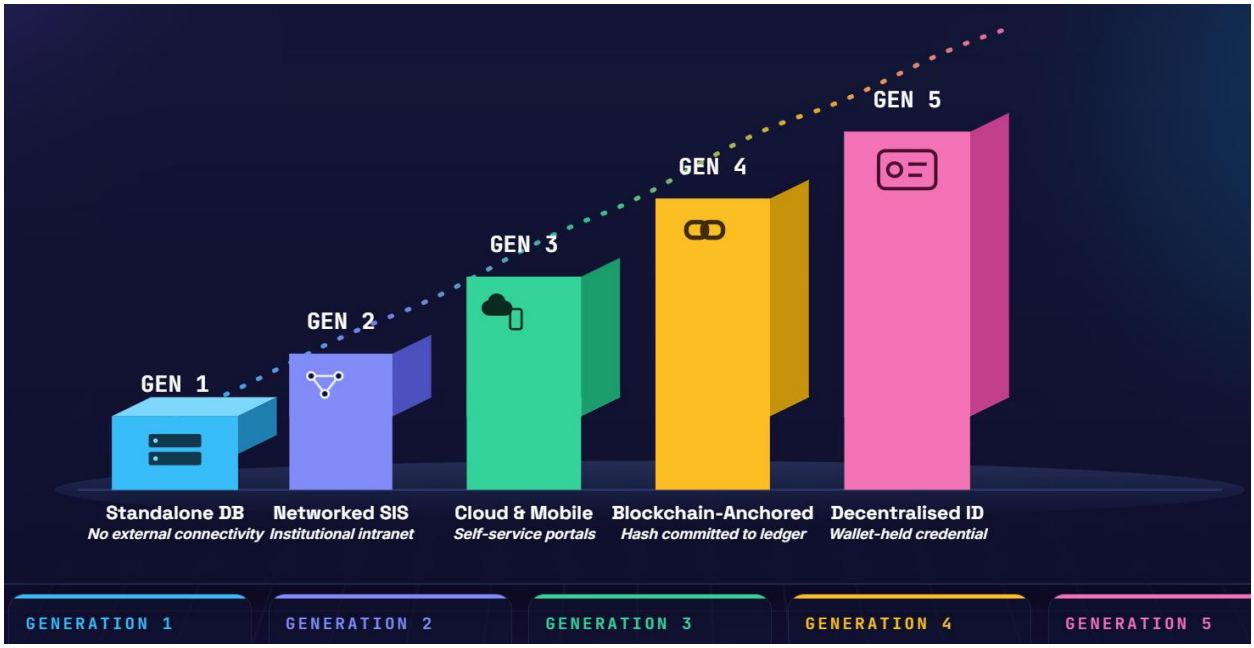

Figure 2: Five generations of computerized record processing

Key Components/Modules of a Typical ERPS

Most contemporary ERPS share four functional modules. The *module for capturing data* receives information from admission forms, grade submissions, or scanned legacy documents. Optical character recognition (OCR) or AI-assisted extraction, are increasingly used for native inputs that are not digital (Ochwo et al., 2018). The *storage module* stores records in a relational NoSQL or hybrid database, often replicated across cloud regions for better preservation. The *verification module* authenticates the identity of requests made and, where applicable; checks the cryptographic integrity of a record, against a stored hash or digital signature. The *distribution module* delivers verified records to students, employers or other institutions (Ibeneme-Sabinus et at., 2020). Typically, this is done via web portals that are secured, application programming interfaces (APIs) or dedicated third-party clearinghouse services. A fifth module, increasingly present in mature deployments, is a *governance and audit module;* which logs every access, modification, and disclosure event for later institutional review and regulatory reporting.

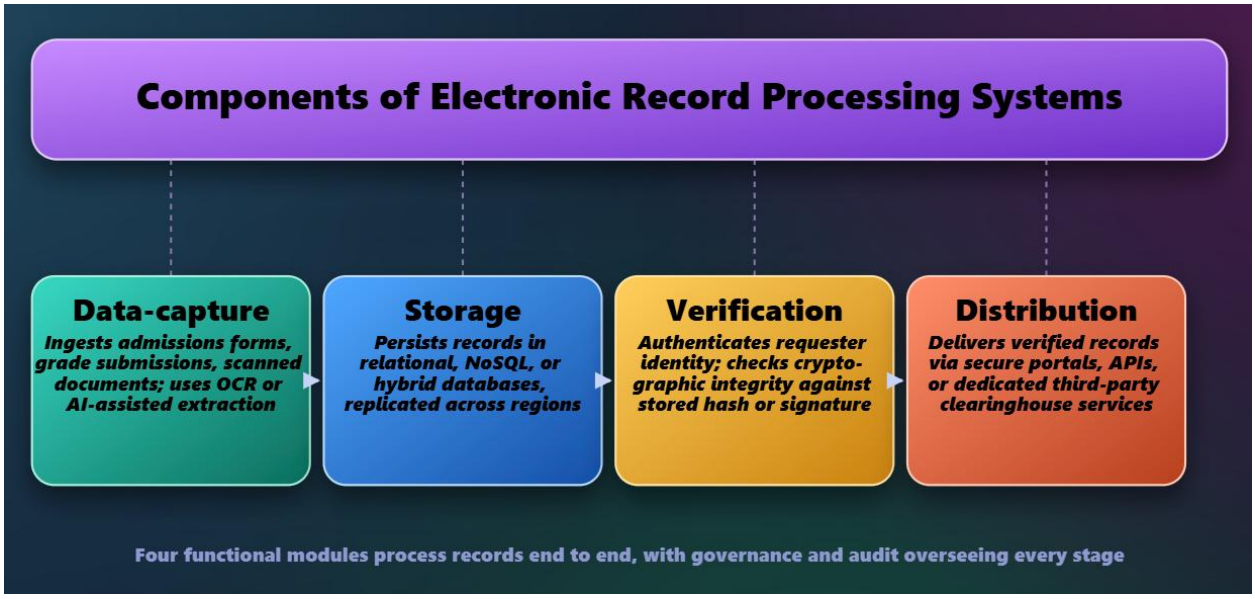

Figure 3: Modules of computerized record processing systems

Stakeholders Involved

- Students and alumni, who require timely, accurate, and portable access to their own records.
- Registrars and institutional administrators, who are responsible for data entry, correction, and governance.
- Receiving institutions and employers, who rely on rapid, trustworthy verification of credentials presented to them.
- Accreditation and verification bodies, which set standards for record content and, in some jurisdictions, operate centralized clearinghouses.
- National examinations councils and admissions boards, which in many countries function as intermediate layer between secondary and tertiary institutions, and are themselves major generators and verifiers of records.
- Regulators and data protection authorities, who enforce compliance with privacy and security law.
- Technology vendors and standard bodies, who supply the platforms and interoperability specifications that institutions build upon rather than developing entirely in-house.

Techniques and Technologies For Record Processing

Database Management Approaches

Relational database management systems (RDBMS) remain the dominant storage paradigm for institutional records because academic data involving students, courses, grades, and enrolments; naturally fits a structured, tabular schema with well-defined relationships and strong transactional guarantees (Bramhanand, 2025). NoSQL systems (document, key-value, or graph stores) are increasingly used alongside relational cores where institutions need to store semi-structured data such as scanned document metadata, activity logs, or flexible curriculum structures that do not map cleanly onto fixed schemas. Hybrid architectures, combining a relational core for authoritative student data (Bramhanand, 2025) with a NoSQL layer for logs and unstructured content, are now common in large-scale student information systems. They are frequently the practical compromise institutions settle on once they outgrow a single-database design but are not prepared to migrate the authoritative student record away from a mature relational platform.

Web-Based and Cloud-Based Architectures

The shift to cloud hosting has allowed institutions to offload infrastructure management to specialized providers, gain elastic scalability during peak periods such as enrolment or graduation; and provide constant self-

service portals to students and third parties (Ibeneme-Sabinus et at., 2020). Software-as-a-Service (SaaS) student-records platforms are common, particularly among smaller institutions that lack technical staff to operate on-premises data centres. Although this shift has also concentrated data-governance responsibility in third-party vendor relationships, that must themselves satisfy institutional compliance obligations.

Blockchain-Based Record Systems

Refers to the use of blockchain, a distributed cryptographically secured digital ledger, as a technique and technology for creating, storing, verifying, and managing records in a way that is: tamper-evident, transparent, and independent of a single controlling authority. A blockchain is a chain of "blocks," each containing a batch of data (records or transactions), a timestamp, and a cryptographic hash of the previous block (Deenmahomed et al., 2020). This chaining has several features that includes distributed ledger, immutability, consensus mechanisms, cryptographic hashing and digital signatures. In immutability, once a record is added, altering it may require changing every subsequent block across majority of the network's copies, making unauthorized tampering computationally impractical. In a distributed ledger, the central server does not hold the official copy alone, many nodes hold copies that are identical; this removes a single point of failure or control. The criteria for making decisions in systems where records are shared, include proof of work, proof of stake, or protocols accessed through permissions (Deenmahomed et al., 2020). These networked systems allow a new block to be added to the chain only when multiple nodes agree. No single participant is able to rewrite the history of blockchain alone. In cryptographic hashing and digital signatures, each record is hashed and signed, which allows anyone to verify whether it is true and original, without relying on a trusted intermediary.

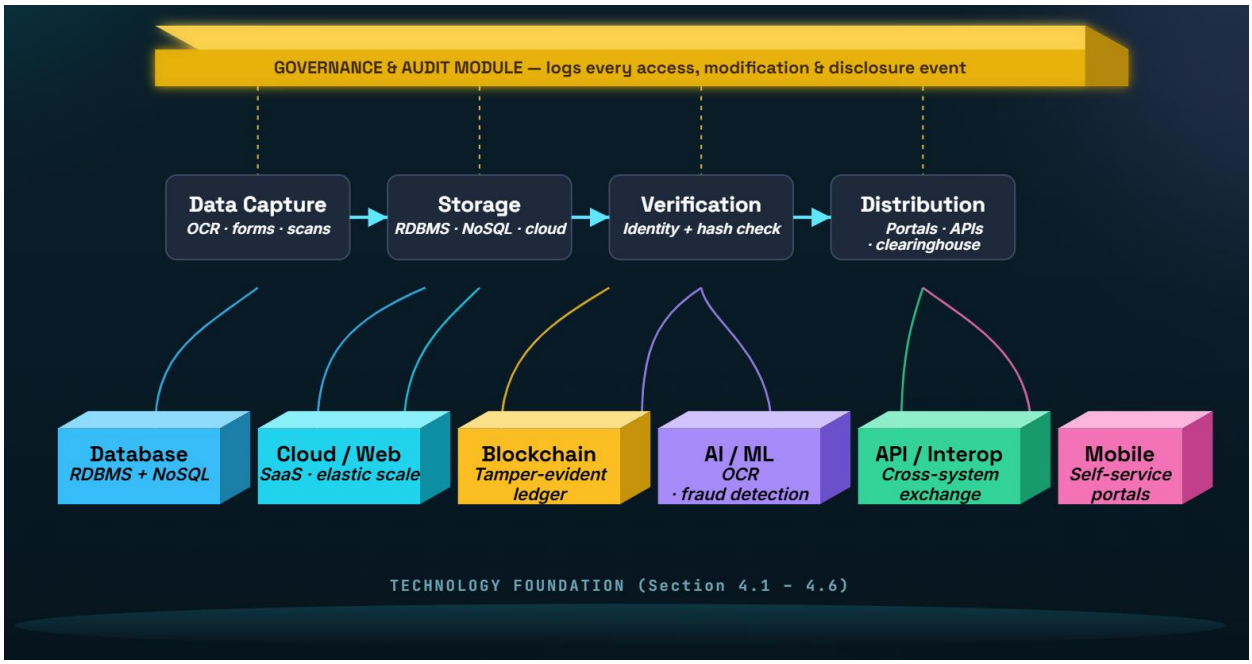

Figure 4: ERPS architecture: from technology foundation to governed workflow

Artificial Intelligence/Machine Learning Applications

These applications are used in ERPS chiefly for two purposes: digitizing legacy paper archives and detecting fraudulent submissions. Optical character recognition (OCR) converts scanned paper transcripts into

machine-readable text, but conventional template-based OCR struggles with the wide variability of transcript layouts across institutions; often requiring a separate template for every source format (Sambetbayeva et al., 2022). However, hundreds of distinct historical transcript layouts exists for large or long-established institutions, and template-maintenance burden frequently offset much of OCR's efficiency benefit. Newer generative AI-based extraction approaches aim to interpret transcript content contextually, rather than matching fixed templates; improving robustness to layout variation and reducing the need for exhaustive template libraries. On the security side, ML-based fraud-detection systems are trained on historical document corpora to flag anomalies in formatting, font, or data-field consistency; that are characteristic of forged or altered documents, complementing rather than replacing cryptographic verification methods (Sambetbayeva et al., 2022).

API-Driven and Interoperability Frameworks

Use application programming interfaces (APIs) and standardized data-exchange architectures to enable different records systems, applications, and organizations: to communicate, share, and process records seamlessly; rather than functioning as isolated, closed silos (Mukred et al., 2019). An *API* is a defined set of rules and protocols that allows one software system to request services or data from another without needing to understand its internal workings. In records processing, APIs act as the "connective tissue" between records management systems (RMS) and enterprise content management (ECM) platforms, line-of-business applications (HR, finance, legal, healthcare systems) and central archives. They also serve government agencies, regulators and external stakeholders who need controlled access to records (Mukred et al., 2019). *Interoperability frameworks* are the broader architectural standards and governance models that ensure these API connections actually produce *meaningful, consistent* data exchange; not just technical connectivity, but shared understanding of formats, metadata, and semantics.

Application to Records Processing

- **Cross-system records capture**: APIs automatically allow ingestion of records into an RMS, directly from the application where they were created (e.g., an email system, ERP, or case management tool), rather than requiring manual export/import.
- **Federated search and retrieval**: Interoperability frameworks let users query records held across multiple, separately-managed repositories through a single interface.
- **Automated metadata harmonization**: APIs map and translate metadata fields from a source system's schema into a receiving system's schema in real time.
- **Records exchange between institutions**: E.g., inter-agency government records transfer, healthcare record sharing between providers (interoperability standards like HL7 FHIR are a close analogue), or supply-chain document exchange between organizations.
- **Integration with emerging technologies**: APIs are typically the mechanism by which records systems connect to blockchain verification layers, AI/ML classification engines, or cloud storage
- **Workflow automation**: Triggering retention/disposal actions, approval routing, or compliance checks automatically, when records cross system boundaries.

Mobile and Self Service Portals

Mobile applications and portals that support web self-service, allow students to request for their transcripts, track application status, and share digital credentials directly from a smartphone, that could be verified; reducing dependence on registrar office opening hours, and postal delivery (Adeleke et al., 2026). This shift has been particularly consequential in regions with large distance-learning populations, where physical access to a campus registrar is impractical. Furthermore, in national examinations contexts, where a single portal must serve millions of candidates simultaneously, around a predictable annual results-release date, rather than a steady year-round trickle of requests.

AJSTME, Volume. 12, Issue 2. 371-387, March, 2026. https://www.ajstme.com.ng
ISSN: 2251-0141 (Print), 2971-6233 (Online)

Table 1: Comparative Analysis of Record Processing Methodologies

Methodology	Strengths	Weaknesses
Relational Database (RDBMS)	Strong consistency; mature tooling; well suited to structured academic data with strict referential rules	Less flexible for unstructured or rapidly changing data models
NoSQL / Hybrid Stores	Flexible schema; scales horizontally for logs, unstructured content, and variable-structure portfolios	Weaker native support for complex relational queries and strict consistency
Cloud/Web Architecture	Elastic scalability; reduced infrastructure burden; always-on self-service	Vendor dependency; data-residency, portability, and third-party compliance concerns
Blockchain-Based Systems	Tamper-evident; verifiable independent of issuer; resistant to forgery	Governance and key-management complexity; limited large-scale longitudinal evidence
Decentralised Identity / Verifiable Credentials	Student-controlled, portable, issuer-signature verification without live database lookup	Shifts key-management burden to individual students; still-maturing tooling and standards uptake
AI/OCR-Based Digitization	Automates legacy archive conversion; assists fraud detection	Accuracy varies with document quality and layout; needs human oversight

Security Frameworks in Record Processing Systems

Common Security Threat

Electronic record processing systems face several known threat categories such as forging of documents (fabrication or alteration of a transcript or certificate), access that was not authorized (credential theft or privilege escalation allowing an attacker to view or alter records), breaches in data (bulk exfiltration of student personal data), and tampering with data in transit or at rest (Ologbosere et al., 2025). Because academic records are frequently used as supporting evidence for employment, immigration, or further study; the incentive for forgery and the downstream harm from a breach are both significant. This holds true, because the same record may be presented as evidence to several independent verifiers over a graduate's lifetime, multiplying the consequences of any single successful forgery.

Authentication and Access Control Mechanisms

Modern ERPS typically implement role-based access control (RBAC) that restricts registrar, faculty, and student users to the minimum data access necessary for their function. Administrative accounts are given multiple factor authentications (MFA), (Ukah et al., 2023). Verification requests from third parties are commonly executed through a controlled portal or clearinghouse, rather than directly accessing the database, limiting the attack surface exposed to external parties.

Encryption Techniques for Data at Rest and in Transit

Encryption at rest (protecting stored database and backup content) and in transit (protecting data moving between client, application, and database tiers, typically via TLS) are now baseline expectations for any cloud-hosted student records system. They are frequently mandated by institutional data-governance policy or contractual terms with hosting vendors (Ibeneme-Sabinus et al., 2020). Backup, and copies recovered from disaster, require the same encryption discipline as production data; since a poorly secured backup may become the weakest link in an otherwise well-secured system.

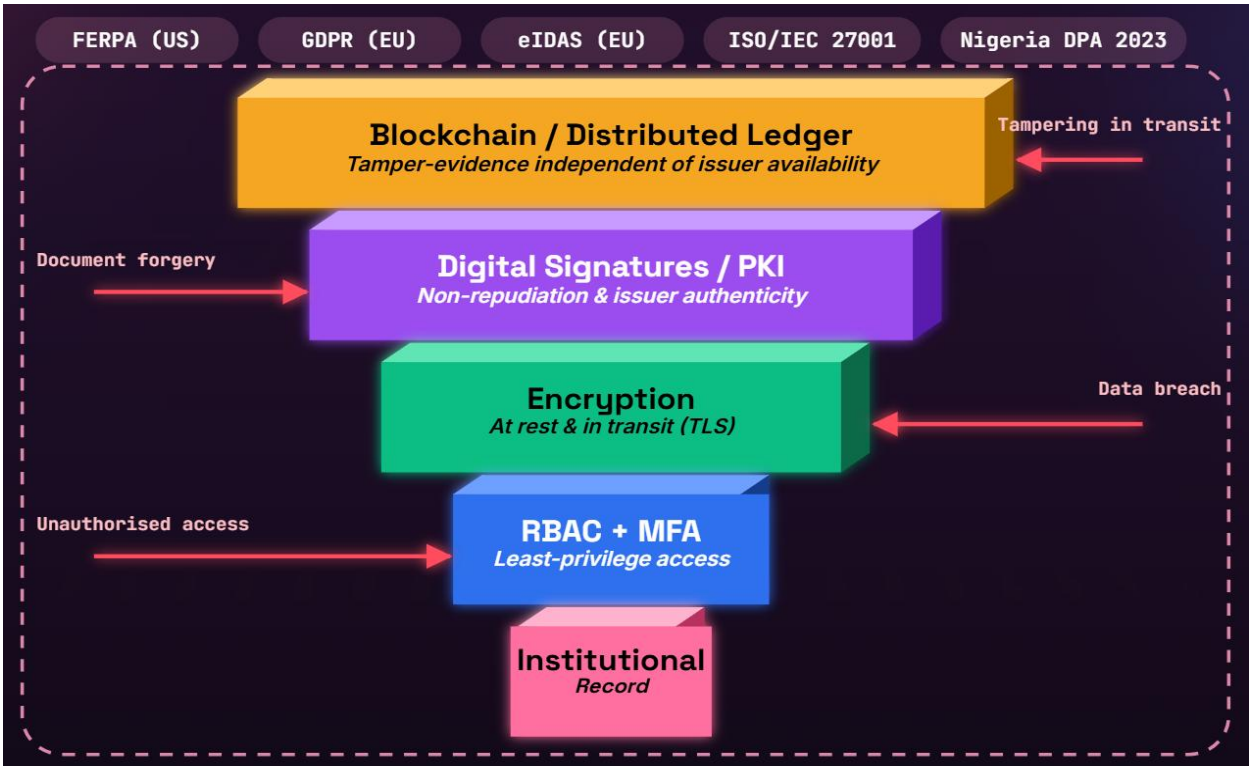

Figure 5: CRPS Security Frameworks: From Threats to Compliance

Digital Signatures and Certificate-Based Verification

Public-key infrastructure (PKI) allows an institution to digitally sign an electronic transcript or certificate, giving a recipient cryptographic assurance that the document originated from the claimed issuer, and has not been altered since signing. No distributed ledger is required (Felisberto et al., 2024). This method is popular with institutions that want proof no one has tampered with data, but without the extra work of setting up and managing a blockchain system. In the European Union, the *electronic identification, authentication and trust services* (eIDAS) regulation provides a harmonized legal framework for electronic signatures, seals, and trust services across member states. They give qualified electronic signatures a status broadly equivalent to handwritten signatures, for cross-border legal and administrative purposes.

Blockchain and Distributed Ledger Security Approaches

Represent the set of cryptographic, architectural and governance mechanisms that blockchain or distributed ledger technology (DLT) systems use to protect the confidentiality, integrity, and availability of records (Hindarto, 2019). Blockchain is not just a record *storage* technique but specifically a *security framework* for records processing systems. This distinguishes it as an approach to answering "how do we keep records safe from tampering,

unauthorized access, and loss?" rather than "how do we structure or exchange records?" Approaches that involves distributed ledger, extend digital signature verification by anchoring a record's hash to a shared ledger, that executes only append operation (Felisberto et al., 2024). Thus, verification no longer depends on the issuing institution remaining reachable or cooperative.

Compliance and Regulatory Standards

In the United States, *the family educational rights and privacy act* (FERPA) governs institutional handling of education records, requiring institutions to limit students' records access, obtain consent before most disclosures, and maintain transparent auditable record-keeping (Katuu, 2016). In the European Union, the *general data protection regulation* (GDPR) imposes comparable but broader obligations on any institution processing the personal data of EU residents. It extends into educational technology vendor relationships, whenever an institution serves EU students; and the related eIDAS regulation separately governs the legal recognition of electronic signatures and trust services. ISO/IEC 27001 provides a widely adopted, certifiable framework for information security management more broadly, and is increasingly referenced in institutional vendor assessment processes alongside FERPA (Katuu, 2016) and GDPR obligations. Nigeria's Data Protection Act 2023 applies to organisations, including national examinations bodies that process the personal data of Nigerian residents, and West Africa's regional examinations council.

Institutional Adoption of Computerized Record Systems

Factors Influencing Adoption

The literature consistently identifies cost, existing infrastructure, institutional policy, staff and student digital literacy, as the principal factors shaping whether and how quickly an institution adopts computerized records systems (Mukred et al., 2019). Resource constrained institutions, particularly in lower income regions, often face a stark trade-off between the up-front cost of new infrastructure and the recurring cost of continued manual processing. Better resourced institutions face different set of adoption barriers, centred on integration with legacy systems already embedded in institutional workflow (Mukred et al., 2019). Leadership commitment has also emerged as a recurring factor: recent cross technology synthesis work on institutional adoption, specifically highlights securing top-management support and building organisational readiness; as central to successful adoption, independent of the specific technology involved.

Adoption Models/Theories Applied in the Literature

At the organizational level, the *technology organization environment* (TOE) framework, originally developed by Tornatzky and Fleisher, explains institutional technology adoption through three interacting contexts. The *technological context* (the complexity, compatibility, and relative advantage of the specific technology under consideration), (Hadwer et al., 2021) the *organizational context* (top-management support, financial resources, and organisational readiness), and the *environmental context* (government policy and regulatory pressure, competitive pressure from peer institutions, and vendor support). A recent cross technology systematic review of TOE applications in higher education technology adoption, found technological complexity, compatibility and relative advantage to be the most frequently documented predictors across a wide range of educational technologies. Organizational top-management support and financial resources are also inclusive, with government policy support, competitive pressure, and vendor partnership; emerging as the dominant environmental factors (Hadwer et al., 2021).

AJSTME, Volume. 12, Issue 2. 371-387, March, 2026. https://www.ajstme.com.ng
ISSN: 2251-0141 (Print), 2971-6233 (Online)

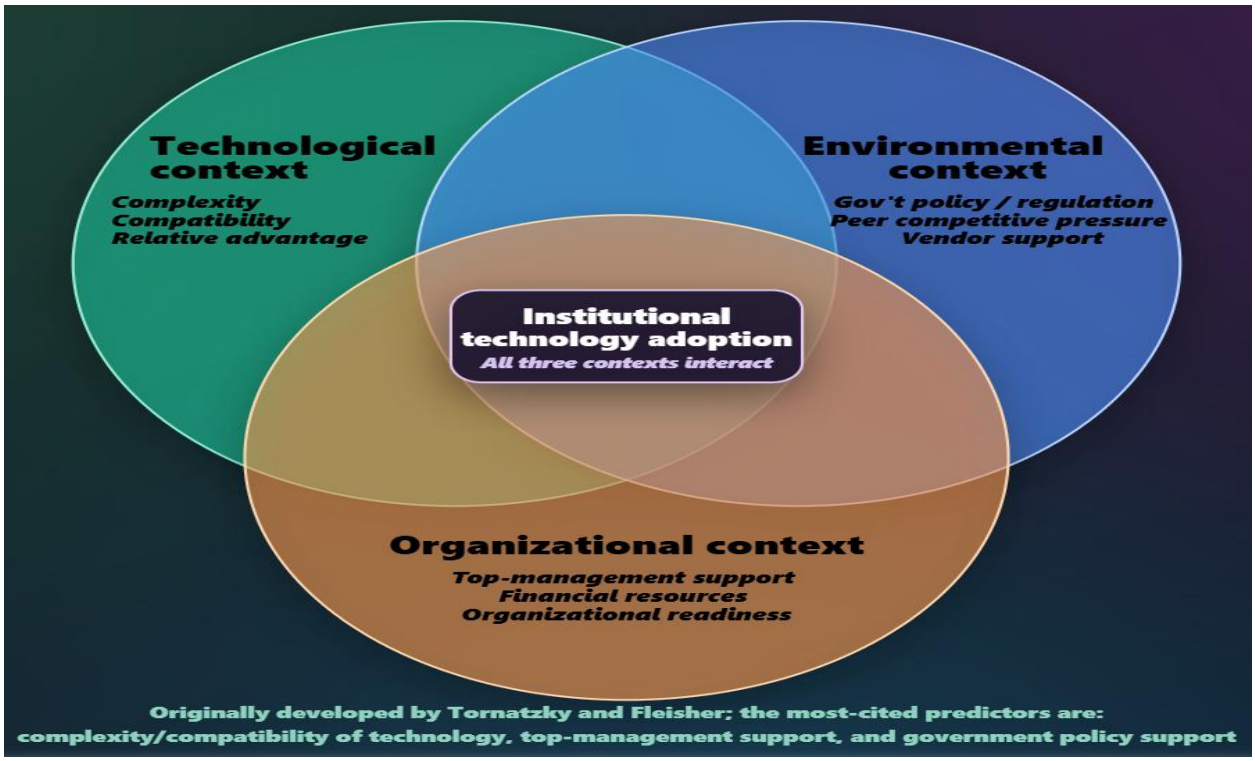

Figure 6: Institutional technology adoption through three interacting contexts

Four theoretical frameworks dominate the institutional adoption literature, operating at two distinct levels of analysis. At the individual user level, *Rogers' diffusion of innovations* theory holds that an innovation's rate of adoption depends on its perceived relative advantage, compatibility with existing values and practices, complexity, trialability, and observability. *Davis's technology acceptance model* (TAM) instead centres on perceived usefulness and perceived ease of use, as primary determinants of a user's intention and attitude to use a new information system. TAM was later extended into TAM2 by Venkatesh and Davis, before Venkatesh and colleagues synthesized constructs from TAM, TAM2, and six further behavioral models; into the *unified theory of acceptance and use of technology* (UTAUT). It is organized around performance expectancy, effort expectancy, social influence, and facilitating conditions.

Table 2: Comparative Evaluation of Security Frameworks

Framework/Mechanism	**Primary Protection Goal**	**Key Limitation**
Role-based access control + MFA	Restrict internal unauthorised access	Depends on rigorous provisioning/deprovisioning discipline
Encryption (at rest/in transit)	Confidentiality of stored and transmitted data	Key-management overhead; does not prevent authorised misuse
Digital signatures/PKI	Non-repudiation and tamper-evidence of issued documents	Requires recipient trust in issuer's public-key infrastructure
Blockchain/distributed ledger	Tamper-evidence independent of issuer availability	Governance complexity; privacy trade-offs on public chains
Decentralised identity / verifiable credentials	Student-controlled portability and issuer-signature verification	Key loss/recovery risk sits with the individual student

Framework/Mechanism	Primary Protection Goal	Key Limitation
eIDAS (EU)	Legal recognition of electronic signatures and trust services	Primarily an EU/EEA legal framework; limited reach elsewhere
FERPA (US)	Legal limits on disclosure of US education records	No certification regime; enforcement via funding sanctions only
GDPR (EU)	Comprehensive personal-data protection and data-subject rights	Broad scope raises compliance cost for global platforms
ISO/IEC 27001	Certifiable information-security management system	Certification does not by itself guarantee sector-specific compliance
National acts (e.g., Nigeria DPA 2023)	Extend baseline data-protection duties to domestic institutions	Enforcement capacity and case law still maturing in many jurisdictions

Table 3: Summary of Reviewed Studies on Institutional Adoption of Computerized Record Processing Systems (CRPS)

Author(s) & Year	Institutional Context	Framework/ Model Used	Research Methods/ Design	System/ Technology Type	Adoption Factors/ Barriers	Key Findings
Oziegbe et al., (2026)	Nigerian tertiary institutions (general, multi-institution review)	No single theoretical model; thematic synthesis of prior ICT-adoption studies	Systematic literature review	Electronic transcript processing systems	Infrastructure deficits, funding constraints, staff ICT competence, resistance to change	Manual transcript processing is slow and error-prone; electronic systems improve speed and accuracy, but adoption remains uneven across Nigerian institutions.
Ahmad (2026)	Postgraduate colleges of Ahmadu Bello University, Zaria	ICT infrastructure assessment approach (no named formal model)	Descriptive survey design	ICT-based student records management infrastructure	Inadequate ICT infrastructure, epileptic power supply, limited staff training, funding	Quality and adequacy of ICT infrastructure significantly influences the effectiveness of student records management.
Adeleke et al., (2026)	Nigerian tertiary institutions (sessional results compilation)	Evaluation of web-based application impact (no named formal model)	Qualitative research design	Web-based results compilation and computation applications	Staff digital literacy, internet connectivity, change-management resistance	Web-based applications improve accuracy, consistency, and turnaround time in compiling and computing students' sessional results.
Ologbosere et al., (2025)	Administrative staff of private universities in Ibadan, Oyo State	Information security awareness framework	Quantitative survey design	Electronic records management systems	Low cybersecurity awareness, inadequate staff training, weak	Higher information security awareness among administrative staff correlates with more

Author(s) & Year	Institutional Context	Framework/ Model Used	Research Methods/ Design	System/ Technology Type	Adoption Factors/ Barriers	Key Findings
					institutional security policy	effective and secure use of electronic records systems.
Okon et al., (2023)	Nigerian universities (academic records units)	Academic Records Maintenance (ARM) practice framework	Descriptive survey / review	Hybrid manual–electronic academic records maintenance systems	Poor funding, unstable power supply, poor ICT skills, lack of standard policy	Many universities still operate hybrid manual/electronic systems; ICT adoption improves record integrity but implementation is inconsistent.
Ukah et al., (2023)	Universities in Cross River State, Nigeria	Availability–accessibility evaluation approach (no named formal model)	Descriptive survey design	Office electronic records management (ERM) systems	Low equipment availability, restricted staff access, poor ICT training	Electronic records systems exist in offices but are not fully accessible or optimally utilized by staff.
Onyekachi et al., (2022)	Tertiary institutions in Rivers State, Nigeria	Records administration effectiveness approach (no named formal model)	Survey research design	Electronic records administration systems	Funding shortfalls, weak infrastructure, low ICT literacy among staff	Proper implementation of electronic records enhances administrative efficiency in tertiary institutions.
Dano et al., (2021)	Tertiary institutions in North-east Nigeria	New Media theory	Descriptive survey design	New/digital media-based records management tools	Regional insecurity, infrastructure deficit, low digital literacy	Adoption of new-media tools improves academic records management despite regional infrastructural and security challenges.
Andreou et al., (2021)	Higher (medical) education institution, cross-sectional study	Comparative exam-proctoring evaluation design	Cross-sectional comparative study	Remote proctoring software vs. on-site proctored examination	Technology reliability, student anxiety/adaptation, equitable access to devices/internet	No significant difference in student exam performance was found between remote and on-site proctored examinations.
Luyombya et al., (2020)	Islamic University in Uganda (private university)	Records management lifecycle model	Case study design	Records management procedures (paper-based and electronic)	Inadequate policy guidelines, insufficient staff training, poor storage facilities	Sound records management procedures are positively linked to improved service delivery.

Author(s) & Year	Institutional Context	Framework/ Model Used	Research Methods/ Design	System/ Technology Type	Adoption Factors/ Barriers	Key Findings
Thong et al., (2020)	University students (curriculum recommendation context)	Transcript-based recommender system model	Data mining / computational modeling design	Data-driven curriculum recommendation system	Data quality/completeness, need for large historical transcript datasets	Analytics derived from student transcripts can generate effective, personalized curriculum recommendations.
Ibeneme-Sabinus et al., (2020)	Tertiary institutions in Nigeria	Encryption-algorithm-based security model	System design and development (software engineering approach)	Web-based document encryption application software	Cybersecurity threats, low institutional awareness of encryption tools	Web-based encryption software enhances confidentiality and security of institutional documents/information.
Deenmahomed et al., (2020)	University education systems (examination, transcript, certification)	Blockchain framework	System design and prototype development	Blockchain-based examination, transcript, and certificate system	High adoption cost, need for cross-institutional collaboration, regulatory acceptance	Blockchain technology can provide tamper-proof, independently verifiable academic records and reduce certificate fraud.
Hindarto (2019)	University enterprise architecture context	Blockchain integrated with enterprise architecture (e.g., TOGAF-style) framework	Enterprise architecture design / case-based approach	Blockchain-based academic identity and transcript management system	Integration complexity, cost of implementation, organizational change management	Embedding blockchain within university enterprise architecture strengthens data integrity and security of identity/transcript records.
Daraghmi et al., (2019)	University academic records access/permission management	Blockchain-based access-control/permission model	System design and prototype development (UniChain)	UniChain blockchain-based records access system	Scalability limitations, adoption cost, building stakeholder trust in new technology	UniChain enables secure, permissioned access to academic records with improved data integrity and tamper resistance.
Mukred et al., (2019)	Higher professional education institutions	Technology–Organization–Environment (TOE)-oriented framework	Conceptual framework development	Electronic Records Management System (ERMS)	Individual competence gaps, technological readiness, weak organizational/	Proposes an integrated framework showing that individual, technological, and environmental factors jointly drive ERMS adoption.

Author(s) & Year	Institutional Context	Framework/ Model Used	Research Methods/ Design	System/ Technology Type	Adoption Factors/ Barriers	Key Findings
			(literature -based)		environmental support	
Omogbhemhea et al., (2018)	Nigerian tertiary institutions (case study: University of Port Harcourt)	Web-based architectural framework	System development / design science approach	Centralized web-based transcript processing system	Cost of implementation, inefficiencies of existing manual system, need for central coordination	A centralized web-based system reduces processing delays and errors and enables remote transcript request and processing.
Ochwo et al., (2018)	Universities in Eastern Uganda	ICT efficacy evaluation approach (no named formal model)	Descriptive survey design	Digitalized student records management systems	Inadequate ICT infrastructure, low staff ICT skills, limited funding	ICT use significantly improves the efficiency and accuracy of digitalized student records management.

Discussion

Research Trends, Theoretical Approaches, and Adoption Barriers in Computerized Record Processing Systems

Table 3 shows that institutional adoption research on computerized record processing systems is dominated by descriptive and quantitative survey designs. Most of the studies reviewed adopted a descriptive survey, quantitative survey, or comparable review-based design; only a small number employed case studies, cross-sectional comparative designs, or system design and prototype development. Geographically, the literature is heavily concentrated in Nigeria, with the remainder drawn from Uganda, Mauritius, Vietnam, and cross-national or general institutional contexts.

A recurring pattern across Table 3 is the absence of a single, named theoretical or conceptual model. In the studies by Oziegbe et al., (2026), Ahmad (2026), Adeleke et al., (2026), Ukah et al., (2023), and Onyekachi et al., (2022); each described their approach as an evaluation or assessment method, rather than an application of a named framework. Where a formal model was used, it came from one of two traditions: technology-adoption theory exemplified by Mukred et al., (2019), Technology-Organization-Environment framework, or blockchain system design exemplified by Deenmahomed et al., (2020), Hindarto (2019), and Daraghmi et al., (2019) This split mirrors the technology-versus-adoption structure of the wider review: some studies modeled why institutions adopt CRPS, while others built and validated the systems themselves.

Despite the diversity of institutional contexts and system types, the adoption barriers reported converge on a small set of recurring factors. These include inadequate ICT infrastructure and unstable power supply (Ahmad, 2026; Okon et al., 2023; Ochwo et al., 2018), funding shortfalls (Oziegbe et al., 2026; Onyekachi et al., 2022), limited staff ICT competence or training (Ukah et al., 2023; Ologbosere et al., 2025), and resistance to change or weak institutional policy (Adeleke et al., 2026; Okon et al., 2023). For blockchain specific systems, the barriers shift toward high adoption cost, scalability, and the need for cross institutional trust and regulatory acceptance (Deenmahomed et al., 2020; Daraghmi et al., 2019). Taken together, the findings in Table 3 consistently report that electronic and blockchain-based systems improve accuracy, consistency, turnaround time, and tamper resistance relative to manual or purely paper-based alternatives; even where full institutional adoption remains incomplete.

Blockchain-Based Frameworks and the Structural Constraints to Institutional Adoption

Strategic frameworks built around blockchain and distributed ledger technology, while technically capable of tamper-evident verification; remain largely confined to system design and prototype studies (Deenmahomed et al., 2020; Hindarto, 2019; Daraghmi et al., 2019), rather than large-scale, longitudinal institutional deployments. The challenges to adoption include poor infrastructures, unstable power supply, less funding, weak policies of institutions, and low staff ICT competence. These were reported in almost the same manner, across studies spanning Nigeria, Uganda, and other contexts for developing countries (Ahmad, 2026; Okon et al., 2023; Dano et al., 2021; Ochwo et al., 2018). This indicates that the adoption of computerized record processing systems by institutions are constrained *less* by the maturity of the technology itself, and *more* from limitations of structures and resources, that lie largely outside the control of individual institutions.

Conclusion

This review has examined computerized record processing systems through two complementary lenses: the technical methodologies and security frameworks that underpin their design, and the empirical evidence on how and why institutions adopt them. The technical literature shows a clear evolutionary trajectory from relational databases toward hybrid, cloud-hosted, and increasingly blockchain-anchored or AI-assisted architectures. Each offers incremental gains in scalability, interoperability and tamper-evidence; matched by a parallel maturing of security frameworks. This includes role-based access control and encryption, digital signatures, distributed ledger verification and an expanding body of data protection regulation (spanning FERPA, GDPR, eIDAS, ISO/IEC 27001, and national instruments such as Nigeria's Data Protection Act 2023). Computerized record systems were consistently found to improve accuracy, consistency, and turnaround time relative to manual alternatives. Nevertheless, institutional adoption remains constrained by infrastructural deficits, funding shortfalls, low staff ICT competence, weak institutional policy, and barriers that recur almost identically across institutional and national contexts.

Recommendations

Based on the findings of this study, it is recommended that:

1. Institutions, especially those with limited resources; should plan and budget for three basic necessities from the very start: reliable internet, backup power, and proper staff training. These should not be treated as optional extras added later, but critical requirements built into the plan from day one, just like the cost of the software itself.
2. Adoption studies should move beyond descriptive surveys, toward quasi-experimental, longitudinal, or comparative designs; capable of supporting causal claims about what drives successful institutional adoption. Future research should use stronger methods that show cause and effect, such as: comparing an institution *before* and *after* it adopts a computerized record system; or comparing similar institutions that use different systems, side by side.
3. Regulators should not stop at passing laws but build systems to enforce them; and create clear, specific guidelines for how records should be handled in different sectors (such as education, health, and government).

References

Asemewalen N. O. & Oziegbe E. T. (2026). Electronic Transcript Processing System For Nigerian Tertiary Institutions; A Systematic Review. *International Journal Of Nature And Science Advance Res.* VOL. 12 NO. 9. DOI: https://doi.org/10.70382/mejnsar.v12i9.089.

Ahmad I. (2026). Ict Infrastructure And Student Records Management In Postraduate Colleges Of Ahmadu Bello University, Zaria. Vol.1, Issue 1, pp.174-183. EISSN 3141-4869.

Adeleke, I. A.; Adegbiji, A. T.; & Abdulrauff, M. F. (2026). Qualitative Impacts Of Web-Based Applications On Students' Sessional Results Compilation And Computation In Tertiary Institutions. *Journal of Educational Studies, Trends and Practice (JESTP)*.Vol. 12, No.8, E-ISSN 3027-1630 P-ISSN 3026-8907. DOI: https://doi.org/10.70382/sjestp.v12i8.099.

Ologbosere A. O. & Abiola V. A. (2025). Information Security Awareness and Effective Use of Electronic Records Systems among Administrative Staff of Private Universities in Ibadan, Oyo State, Nigeria. *International Journal of Research and Innovation in Social Science (IJRSS)*. ISSN No. 24546186.Volume IX. Issue XIV. https://doi.org/10.47772/IJRSS.

Okon G., Umoren E. E. & Kathryn P. (2023). Academic Records Maintenance (ARM) in Nigerian Universities. Library Philosophy and Practice (e-journal). 7936. https://digitalcommons.unl.edu/libphilprac/7936.

Ukah T. A. & Azih N. (2023). Extent of Availability and Accessibility of Office Electronic Records Management in Universities in Cross River State, Nigeria. Academic Journal of Current Research Vol.10, No.1; January-2023; ISSN (2343 – 403X); p –ISSN 3244 – 5621.

Onyekachi N. E. & Nwereka W. E. (2022). Electronic Records and Administration of Educational Tertiary Institutions in Rivers State. *African Journal of Humanities & Contemporary Education Research.* Vol. 3, No. 1.ISSN: 2760-5689X.

Dano A. I. & Ibrahim M. M. (2021). Management of Students' Academic Records in Tertiary Institutions in North-east Nigeria: The New Media Imperative. Library Philosophy and Practice (e-journal) 5483. https://digitalcommons.unl.edu/libphilprac/5483.

Andreou V., Peters S., Eggermont J., Johan W. & Schoenmakers B. (2021). Remote versus on-site proctored exam: comparing student results in a cross-sectional study. *BMC Medical Education* 21:624 https://doi.org/10.1186/s12909-021-03068-x.

Luyombya D. & Ndagire S. (2020). Records management procedures and service delivery in private universities: a case study of the Islamic University in Uganda. Journal of SASA. Volume 53, 2020. ISSN: 1012-2796. https://dx.doi.org/10.4314/jsasa.v53i1.1.

Thong M., Chung N. T., Thanh V. & Thoai N. (2020). From Transcripts to Insights for Recommending the Curriculum to University Students. *SN Computer Science* (2020) 1:323 https://doi.org/10.1007/s42979-020-00332-7.

Ibeneme-Sabinus I. L.., Amadi E. C., Ekedebe N., Nwokonkwo O., Ibeneme-Sabinus I. & Ajah B. O. (2020). A Web Based Document Encryption Application Software for Information Security in Tertiary Institutions. *Journal of Cybersecurity and Information Management (JCIM).* Vol. 4, No. 1, PP. 26-35. https://doi.org/10.5281/zenodo.3909971.

Deenmahomed H. A|. M., Didier M.M. & Sungkur R. K. (2020). The future of university education: Examination, transcript, and certificate system using blockchain. *Comput Appl Eng Educ.* 2021;1–23. *Wiley Periodicals.* https://doi.org/10.1002/cae.22381.

Hindarto D. (2019). Blockchain-Based Academic Identity and Transcript Management in University Enterprise Architecture. *Sinkron : Jurnal dan Penelitian Teknik Informatika.* Volume 7, Number 4. e-ISSN : 2541-2019 p-ISSN : 2541-044X. https://doi.org/10.33395/sinkron.v8i4.12978.

Daraghmi E., Daraghmi Y. & Yuan S. (2019). UniChain: A Design of Blockchain-Based System for Electronic Academic Records Access and Permissions Management. Applied Sciences 9, 4966; https://doi.org/doi:10.3390/app9224966.

Mukred M., Yusof Z. M., Mokhtar U. A. & Fauzi F. (2019). A Framework for Electronic Records Management System Adoption in the Higher Professional Education: Individual, Technological and Environmental Factors. *Springer Nature IRICT* 2018, AISC 843, pp. 840–849. https://doi.org/10.1007/978-3-319-99007-1_78.

Omogbhemhea M. & Akpojaro J. (2018). Development of Centralized Transcript Processing System. *American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)* ISSN (Print) 2313-4410, ISSN (Online) 2313-4402.

Ochwo D., Atibuni D. Z. & Sekiwu D. (2018). Efficacy of information and communication technology in digitalized students' records management in universities in Eastern Uganda. *African Educational Research Journal* Vol. 6(2), pp. 99-106. ISSN: 2354-2160. https://doi.org/10.30918/AERJ.62.18.009.