Design and Implementation of a Secure NFC-Based Attendance System with Role-Aware Access Control and Verifiable Audit Trails

Ifeanyichukwu Uchechukwu Akpara[1]; Otugene Victor Bamigwojo[2];
Lawrence Anebi Enyejo[3]; Gamaliel Ibuola Olola[4]

[1]Department of Computer Science, Prairie View A&M University, Prairie View, Texas, USA
[2]Department of Mathematics, Federal University, Lokoja
[3]Telecommunications and Ancillary Unit. NBC HQ. Abuja, Federal Capital Territory, Nigeria.
[4]Canadore College, Canada Duke Street, North Bay, ON

Publication Date: 2026/03/30

Abstract: Secure and verifiable attendance management systems are essential in institutional environments where identity assurance, authorization control, and audit accountability are critical. Conventional attendance solutions based on manual registers, static RFID identifiers, or standalone biometric systems suffer from replay vulnerabilities, cloning risks, weak authorization enforcement, and non-verifiable logging mechanisms. This study proposes and experimentally validates a Secure NFC-Based Attendance System integrating mutual authentication using nonce-based protocols, a Role-Aware Access Control (RAAC) model, and a cryptographically verifiable audit trail framework.

The proposed authentication protocol employs dual nonce exchange and AES-256 encryption to achieve replay resistance and cloning protection, with attack success probability bounded by $1/2^n$ for n-bit nonces. The RAAC model extends classical RBAC by incorporating contextual constraints such as time and locationinto a formally defined authorization function, ensuring context-sensitive privilege enforcement and preventing unauthorized role activation. Audit integrity is guaranteed through hash-chain logging, where each record is cryptographically linked to its predecessor, providing forward-security and tamper-evidence with collision resistance bounded by $1/2^{256}$.

Experimental evaluation using 13.56 MHz NFC hardware and a simulated institutional dataset demonstrates low authentication latency (mean < 15 ms), constant-time authorization complexity, and scalable throughput exceeding operational benchmarks. Security analysis confirms strong resistance against replay, relay, cloning, privilege escalation, and log tampering attacks.

The results establish that robust cryptographic authentication, formalized authorization logic, and verifiable audit mechanisms can be integrated without compromising real-time performance. The framework provides a scalable and compliance-ready solution for secure attendance management in academic and enterprise environments.

Keywords: *Secure NFC Authentication; Role-Aware Access Control (RAAC); Hash-Chain Audit Logging; Tamper-Evident Systems; Performance–Security Trade-Off.*

How to Cite: Ifeanyichukwu Uchechukwu Akpara; Otugene Victor Bamigwojo; Lawrence Anebi Enyejo; Gamaliel Ibuola Olola (2026) Design and Implementation of a Secure NFC-Based Attendance System with Role-Aware Access Control and Verifiable Audit Trails. *International Journal of Innovative Science and Research Technology*, 11(3), 2503-2523. https://doi.org/10.38124/ijisrt/26mar1769

I. INTRODUCTION

➢ *Background and Motivation*

Attendance management systems are foundational components of institutional governance, workforce accountability, and academic performance monitoring. Traditionally, attendance recording has relied on manual logbooks and signature sheets, which are susceptible to proxy attendance, transcription errors, delayed reporting, and limited audit traceability (Khan et al., 2020). Manual systems also lack cryptographic binding between identity and transaction events, making them unsuitable for environments requiring high-integrity records. Although Radio Frequency Identification (RFID) systems introduced automation, many implementations operate without strong cryptographic authentication, exposing them to tag cloning, spoofing, and unauthorized credential duplication (Avoine et al., 2017; Juels, 2006). Consequently, RFID-based attendance mechanisms without secure key management remain vulnerable to impersonation attacks and data tampering.

Biometric attendance systems, including fingerprint and facial recognition technologies, attempt to mitigate identity spoofing but introduce significant privacy and data protection concerns. Biometric identifiers are inherently sensitive and immutable; once compromised, they cannot be revoked or reissued (Jain et al., 2016). Regulatory frameworks such as the General Data Protection Regulation (GDPR) emphasize data minimization, purpose limitation, and secure processing of personally identifiable information (European Parliament & Council, 2016). The storage of biometric templates in centralized databases increases exposure to data breaches and raises ethical and compliance risks (Ratha et al., 2001). These concerns motivate the exploration of secure yet privacy-preserving alternatives such as Near Field Communication (NFC).

NFC, standardized under ISO/IEC 14443 and related proximity card specifications, offers short-range communication (typically <10 cm) and supports cryptographic primitives such as AES-based mutual authentication (Haselsteiner & Breitfuß, 2006). Its constrained operational range reduces certain remote interception risks compared to conventional RFID. However, NFC-based systems are not immune to adversarial exploitation. Relay attacks extend communication channels beyond intended physical proximity, effectively bypassing distance constraints (Hancke, 2005). Tag cloning and replay attacks exploit weak authentication protocols or predictable challenge–response exchanges, enabling unauthorized attendance registration (Avoine et al., 2017; Francillon et al., 2011). Without nonce-based session validation and secure key derivation, NFC deployments may inherit vulnerabilities similar to legacy RFID systems.

Beyond identity authentication, institutional environments demand differentiated authorization structures. Universities and corporate organizations operate with hierarchical and functional role distributions students, lecturers, administrators, system auditors each requiring distinct privileges. Classical Role-Based Access Control (RBAC) models formalize authorization by mapping users to roles and roles to permissions (Sandhu et al., 1996). However, static RBAC models may not sufficiently address contextual conditions such as time constraints, physical location, or device trust level (Hu et al., 2015). For example, attendance validation rights for lecturers should be active only within scheduled instructional periods and designated venues. Thus, there is a need for role-aware access control mechanisms that integrate contextual constraints into authorization decisions.

Equally critical is the requirement for verifiable auditability. Attendance records often serve as evidence in disciplinary actions, accreditation assessments, payroll processing, and compliance reporting. Therefore, tamper-evident logging mechanisms must ensure data integrity and non-repudiation. Cryptographic hash chaining and secure logging frameworks provide mathematical guarantees of record immutability by linking each entry to its predecessor (Schneier & Kelsey, 1999). Any alteration of a historical record invalidates subsequent hashes, enabling detection of manipulation. In regulated environments, such mechanisms support accountability, forensic analysis, and policy enforcement.

Modern compliance regimes increasingly demand traceable and verifiable digital records. Standards such as ISO/IEC 27001 emphasize secure information management, integrity protection, and access accountability (ISO/IEC, 2013). Institutions are expected to demonstrate that attendance data cannot be altered retroactively without detection. This requirement extends beyond data confidentiality to integrity assurance and audit transparency. Consequently, a secure NFC-based attendance system must integrate strong cryptographic authentication, role-aware authorization logic, and mathematically verifiable audit trails. Previous studies have shown that decision support systems driven by data analytics can significantly enhance manufacturing productivity by optimizing operational workflows and reducing waste (Jalloh & Bamigwojo, 2023).

In summary, while NFC technology presents a promising foundation for automated attendance systems, secure deployment necessitates addressing three interrelated dimensions: (1) robust cryptographic authentication resistant to relay, replay, and cloning attacks; (2) context-aware, role-sensitive authorization models; and (3) tamper-evident logging mechanisms aligned with regulatory compliance standards. The convergence of these requirements forms the technical motivation for the present research.

➢ *Problem Statement*

Despite the growing adoption of Near Field Communication (NFC) technologies in automated attendance systems, many implementations remain architecturally insecure and lack formal security guarantees. Existing deployments frequently rely on static identifier transmission or weak challenge–response mechanisms without cryptographic binding between the NFC tag and backend verification server (Avoine et al., 2017; Juels, 2006). In such configurations, the absence of mutual authentication protocols exposes the system to replay attacks, cloning, and man-in-the-middle relay exploits (Hancke, 2005; Francillon et al., 2011). Without secure nonce generation and session key derivation, authentication cannot be mathematically validated against adversarial replay probability models. Consequently, attendance transactions may be fraudulently injected into the system without detection, undermining institutional trust and accountability.

A further limitation concerns the absence of rigorously defined authorization logic. While some attendance platforms implement basic user categorization (e.g., student vs. administrator), these classifications are typically enforced through static database flags rather than formally modeled access control structures (Sandhu et al., 1996). The lack of mathematically grounded role-based authorization prevents formal verification of policy consistency and completeness. Classical Role-Based Access Control (RBAC) models define relationships among users, roles, and permissions through set-theoretic mappings, enabling provable enforcement guarantees (Ferraiolo et al., 2001). However, many NFC attendance systems do not implement such formal mappings, nor do they incorporate contextual constraints such as temporal validity or spatial authorization (Hu et al., 2015). In the absence of a mathematically defined authorization function, the system cannot be subjected to formal access verification, thereby increasing the risk of privilege escalation and unauthorized administrative overrides.

Equally problematic is the lack of verifiable and immutable audit trails. Attendance records often serve evidentiary purposes in accreditation reviews, payroll processing, compliance audits, and disciplinary proceedings. Yet, numerous implementations rely on conventional database logging mechanisms that permit retrospective modification by privileged insiders (Schneier & Kelsey, 1999). Without cryptographic integrity protection, log entries remain vulnerable to alteration or deletion without detectable trace. Secure logging research demonstrates that tamper-evident mechanisms such as hash chaining, forward-secure logging, and cryptographic timestamping provide mathematical guarantees that any modification to historical records is computationally detectable (Bellare & Yee, 1997; Crosby & Wallach, 2009). In contrast, unsecured audit tables lack collision-resistant linking structures, preventing reliable forensic verification.

From a compliance perspective, regulatory frameworks such as ISO/IEC 27001 emphasize integrity, accountability, and traceability in information systems (ISO/IEC, 2013). Systems that cannot demonstrate verifiable immutability of records fail to meet modern governance expectations. Furthermore, data protection regulations require demonstrable safeguards against unauthorized alteration of personally identifiable information (European Parliament & Council, 2016). An attendance system that cannot produce cryptographically verifiable proof of transaction integrity may therefore fall short of institutional and legal audit standards.

The convergence of these deficiencies (1) absence of cryptographic verification in NFC authentication workflows, (2) lack of formally modelled role-based authorization logic, and (3) non-verifiable audit logging architectures constitutes a critical research gap. Current implementations do not integrate authentication security, authorization rigor, and tamper-evident accountability within a unified mathematical framework. Without such integration, attendance systems remain susceptible to identity fraud, privilege misuse, and undetectable data manipulation.

Accordingly, there exists a pressing need for a secure NFC-based attendance architecture that incorporates formally defined cryptographic authentication protocols, mathematically modelled role-aware access control mechanisms, and verifiable, immutable audit trails grounded in cryptographic hash structures. Addressing this gap forms the central problem this study seeks to resolve.

➢ *Objectives*

The overarching objective of this study is to design and validate a secure, scalable, and verifiable NFC-based attendance system that integrates cryptographic authentication, formally defined role-aware authorization logic, and tamper-evident audit trails within a unified architectural framework.

- *Objective 1: Design a Cryptographically Secure NFC Attendance Framework*

The first objective is to construct a secure NFC authentication protocol that ensures confidentiality, integrity, and authenticity of attendance transactions. Let U denote the set of registered users and T the set of NFC tags associated with those users. The authentication mechanism must guarantee that for any attendance transaction τ, the probability of successful impersonation satisfies:

$$P(\text{Impersonation}) \leq \frac{1}{2^k}$$

Where k represents the effective cryptographic key length.

The system shall incorporate mutual authentication using nonce-based protocols such that for each session:

$$K_s = H(K_t \parallel N_r \parallel N_t)$$

Where:

K_t is the tag-specific secret key,

N_r and N_t are reader and tag nonces respectively,

$H(\cdot)$ is a collision-resistant hash function.

This ensures freshness, replay resistance, and session key uniqueness.

- *Objective 2: Implement a Role-Aware Access Control (RAAC) Model*

The second objective is to formalize a role-aware authorization framework extending classical RBAC with contextual constraints.

Let:

U = set of users

R = set of roles

P = set of permissions

C = set of contextual attributes

User-role assignment:

$$UA \subseteq U \times R$$

Role-permission assignment:

$$PA \subseteq R \times P$$

The authorization decision function is defined as:

$$Access(u,p,c) = \begin{cases} 1 & \text{if } \exists r \in R: (u,r) \in UA \wedge (r,p) \in PA \wedge f(c) = 1 \\ 0 & \text{otherwise} \end{cases}$$

Where $f(c)$ enforces contextual constraints such as time validity, device trust level, and physical location.

This objective ensures mathematically verifiable authorization logic and prevents privilege escalation.

- *Objective 3: Develop a Verifiable Audit Trail Mechanism Using Hash Chaining*

The third objective is to implement a tamper-evident logging mechanism grounded in cryptographic hash chaining.

For each attendance record R_i, the log hash is computed as:

$$H_i = H(H_{i-1} \parallel R_i)$$

Integrity condition:

$$Integrity = 1 \iff H_n^{recomputed} = H_n^{stored}$$

This guarantees that any modification to historical records invalidates the chain, thereby enabling provable immutability and forensic verifiability.

- *Objective 4: Evaluate Performance, Security, and Scalability*

The final objective is to empirically assess:

- ✓ Authentication latency L_a
- ✓ Authorization decision time L_{auth}
- ✓ Audit verification time L_v
- ✓ System throughput

Throughput is modelled as:

$$Throughput = \frac{N}{T_{processing}}$$

Where N represents the number of attendance transactions processed within time interval $T_{processing}$.

Security evaluation includes replay resistance probability and entropy analysis of credential identifiers.

➢ *Contributions*

This study makes four primary contributions to secure NFC-based identity systems:

- *A Secure NFC Authentication Protocol with Nonce-Based Mutual Authentication*

We propose a cryptographically robust NFC protocol incorporating:

- ✓ Dynamic nonce exchange
- ✓ Session key derivation
- ✓ AES-based encryption
- ✓ Replay detection

The protocol satisfies mutual authentication and freshness properties under standard adversarial models.

- *A Formalized Role-Aware Access Control (RAAC) Model*

The research introduces a mathematically defined RAAC framework that:

- ✓ Extends RBAC with contextual constraints
- ✓ Supports dynamic role activation
- ✓ Enables formal verification of authorization logic
- ✓ Reduces privilege misuse risks

The model provides provable authorization correctness using set-theoretic mapping.

- *A Hash-Linked Verifiable Audit Logging Framework*

We design a forward-secure logging mechanism using cryptographic hash chaining. The framework ensures:

- ✓ Tamper-evident attendance records
- ✓ Non-repudiation of transactions
- ✓ Integrity validation through recomputation
- ✓ Forensic traceability

This architecture supports compliance with institutional and regulatory auditing requirements.

- *Experimental Validation Under Realistic Deployment Conditions*

The proposed system is implemented and evaluated using real NFC hardware (13.56 MHz readers) and a secure backend environment. Performance metrics—including authentication latency, throughput, and scalability—are measured under simulated institutional workloads. Security robustness is assessed against replay, cloning, and privilege escalation attack scenarios.

Together, these contributions establish a unified cryptographic, authorization, and audit framework for secure NFC-based attendance systems suitable for deployment in security-sensitive institutional environments.

II. LITERATURE REVIEW

➢ *NFC Security Architectures*

Recent advancements in secure attendance systems emphasize the integration of cryptographic authentication, contextual authorization, and verifiable audit mechanisms within unified architectures. Traditional NFC and RFID-based systems often rely on static identifiers or weak challenge–response protocols, making them vulnerable to replay, cloning, and impersonation attacks. Emerging frameworks address these limitations by incorporating mutual authentication using nonce-based protocols and strong encryption schemes to ensure session integrity and identity assurance (Usoro, et al., 2025). For instance, a secure NFC-based architecture integrating AES-driven authentication with role-aware access control and hash-linked audit trails demonstrates improved resistance to adversarial exploits while maintaining low latency and high throughput (Akpara et al., 2026).

Furthermore, the evolution of access control models from static RBAC toward context-aware authorization has significantly improved system resilience against privilege misuse. By embedding temporal, spatial, and device-level constraints into authorization functions, modern systems enforce dynamic policy validation and reduce unauthorized access risks. In addition to authentication and authorization, secure audit logging has become a critical requirement for institutional compliance and forensic accountability. Cryptographic hash chaining and forward-secure logging mechanisms ensure tamper-evident recordkeeping, thereby aligning with global information security standards. The growing recognition of such integrated approaches within the academic and professional community further underscores their relevance, as reflected in peer-review excellence and scholarly contributions acknowledged through international awards.

Near Field Communication (NFC) is a short-range wireless communication technology operating at 13.56 MHz and standardized primarily under the ISO/IEC 14443 proximity card specifications. ISO/IEC 14443 defines the physical characteristics, radio frequency power and signal interface, initialization and anti-collision protocols, and transmission protocols for contactless smart cards (ISO/IEC, 2018). The standard supports half-duplex communication between a reader (Proximity Coupling Device, PCD) and a tag (Proximity Integrated Circuit Card, PICC), typically within a range of 4–10 cm. While this limited operational range is often perceived as an inherent security advantage, it does not eliminate adversarial risks, particularly when cryptographic safeguards are weak or improperly implemented (Haselsteiner & Breitfuß, 2006).

Modern NFC deployments increasingly incorporate cryptographic authentication mechanisms to strengthen identity verification and data confidentiality. Advanced implementations rely on symmetric-key algorithms such as the Advanced Encryption Standard (AES) for challenge–response authentication and session key derivation (Avoine et al., 2017). In such schemes, a shared secret key K is stored securely on both the tag and backend system. Mutual authentication is achieved through encrypted nonce exchange, ensuring freshness and replay resistance. In more security-sensitive environments, elliptic curve cryptography (ECC) is adopted to enable asymmetric key-based authentication while maintaining computational efficiency suitable for resource-constrained NFC chips (Juels, 2006). ECC-based schemes reduce key size requirements while preserving high security margins, making them particularly attractive for embedded contactless systems.

Despite these advancements, NFC systems remain susceptible to well-documented vulnerabilities. Replay attacks occur when an adversary intercepts a legitimate authentication exchange and retransmits it to gain unauthorized access. Without proper nonce validation and timestamp verification, the probability of successful replay remains non-negligible (Avoine et al., 2017). Relay attacks, also referred to as “mafia fraud” attacks, extend the communication channel between a legitimate tag and reader over a longer distance than intended, effectively bypassing physical proximity constraints (Hancke, 2005). Experimental demonstrations have shown that ISO/IEC 14443-based systems can be exploited through real-time relaying, undermining assumptions of spatial security.

Tag cloning represents another critical vulnerability. When static identifiers (UIDs) are transmitted without cryptographic protection, attackers can duplicate tag credentials and emulate legitimate users (Juels, 2006). Even in systems employing cryptographic primitives, weak key management or predictable authentication sequences may enable extraction or inference of secret keys. Francillon et al. (2011) demonstrated that poorly protected contactless systems are vulnerable to practical relay-based impersonation attacks, emphasizing the need for mutual authentication and session-specific cryptographic binding.

The literature therefore establishes that while ISO/IEC 14443 provides a standardized communication framework, security is not guaranteed at the protocol level alone. Robust NFC security architectures must integrate strong cryptographic primitives (e.g., AES-128/256, ECC), mutual authentication using nonce-based protocols, secure key storage, and replay-resistant session management. Absent these mechanisms, NFC-based identity systems including attendance platforms remain exposed to cloning, relay, and replay threats.

In summary, prior research highlights both the potential and the limitations of NFC security architectures. Although cryptographic implementations significantly enhance protection, vulnerabilities persist when authentication protocols are improperly designed or when systems rely solely on physical proximity assumptions. These findings underscore the necessity of a rigorously engineered cryptographic framework in secure NFC-based attendance systems.

➢ *Role-Based Access Control (RBAC) and Extensions*

Role-Based Access Control (RBAC) remains one of the most widely adopted authorization paradigms for structured organizational environments. The classical RBAC model formalizes authorization through well-defined relationships among users, roles, and permissions (Sandhu et al., 1996). Its mathematical structure enables precise specification, policy verification, and enforcement consistency, making it particularly suitable for institutional systems requiring hierarchical control and separation of duties.

- *Formally, Let:*

- ✓ U denote the set of users,
- ✓ R denote the set of roles,
- ✓ P denote the set of permissions,
- ✓ $UA \subseteq U \times R$ represent the user–role assignment relation,
- ✓ $PA \subseteq R \times P$ represent the role–permission assignment relation.

Under the classical RBAC model, the access decision function is defined as:

$$Access(u,p) = \begin{cases} 1 & \text{if } \exists r \in R: (u,r) \in UA \wedge (r,p) \in PA \\ 0 & \text{otherwise} \end{cases}$$

This formulation ensures that a user u is granted permission p only if there exists a role r such that u is assigned to r and r is authorized for p. The separation of user-role and role-permission mappings simplifies policy administration and supports the principle of least privilege (Ferraiolo et al., 2001). Moreover, RBAC models facilitate hierarchical role inheritance, enabling structured delegation across organizational levels.

Despite its strengths, classical RBAC assumes static assignment relationships and does not inherently incorporate environmental or contextual attributes. In dynamic operational environments such as NFC-based attendance systems authorization decisions often depend on contextual factors including time validity, device trust level, geographic location, and session integrity (Usoro, & Amunigun, 2024). For instance, a lecturer's permission to validate attendance may be constrained to scheduled instructional hours, while administrative privileges may require access from trusted institutional devices.

To address these limitations, RBAC has evolved toward context-aware and attribute-augmented models. The National Institute of Standards and Technology (NIST) extended RBAC to include constraint mechanisms such as temporal restrictions and separation-of-duty policies (Ferraiolo et al., 2001). More recent approaches integrate contextual attributes directly into the authorization decision process, bridging RBAC with Attribute-Based Access Control (ABAC) concepts (Hu et al., 2015). In such extensions, the access decision becomes a function not only of role membership but also of contextual variables $c \in C$:

$$Access(u,p,c) = \begin{cases} 1 & \text{if } \exists r \in R: (u,r) \in UA \wedge (r,p) \in PA \wedge f(c) = 1 \\ 0 & \text{otherwise} \end{cases}$$

Here, $f(c)$ represents a contextual validation function evaluating constraints such as:

$$f(c) = \mathbb{1}(t \in T_{allowed}) \cdot \mathbb{1}(device = trusted)$$

Where $\mathbb{1}(\cdot)$ denotes the indicator function.

Research has demonstrated that incorporating contextual constraints significantly reduces insider threat risk and privilege misuse, particularly in systems where authorization decisions are sensitive to operational conditions (Bertino et al., 2001). Furthermore, dynamic RBAC models improve resilience against credential compromise by restricting privilege activation based on situational trust evaluation (Kuhn et al., 2010).

In secure NFC-based attendance systems, the integration of RBAC with contextual enforcement is critical. Merely assigning static roles to users is insufficient to prevent misuse if contextual verification is absent (Sanmori, 2024). For example, an administrator credential cloned via an NFC attack could be exploited unless role activation is bounded by time, location, or device integrity conditions. Therefore, extending classical RBAC with contextual constraints ensures mathematically verifiable authorization while maintaining operational flexibility.

In summary, the RBAC model provides a rigorous foundation for role-based authorization through formally defined set relationships and decision functions. However, contemporary security-sensitive applications necessitate contextual augmentation to address dynamic operational risks. The integration of contextual constraints into RBAC forms a robust authorization framework capable of supporting secure NFC-based attendance infrastructures.

➢ *Secure Audit Logging Mechanisms*

Secure audit logging constitutes a foundational requirement for systems that must provide verifiable integrity, non-repudiation, and forensic accountability. In security-sensitive infrastructures such as identity and attendance systems, audit records are not merely operational metadata; they function as evidentiary artifacts subject to institutional review, regulatory inspection, and dispute resolution. Conventional database logging mechanisms, however, permit privileged modification, deletion, or retroactive alteration without cryptographic detection, thereby undermining evidentiary reliability (Schneier & Kelsey, 1999). Secure audit logging research addresses this vulnerability through mathematically verifiable integrity structures.

- *Hash-Chain-Based Logging*

One of the most widely adopted tamper-evident mechanisms is cryptographic hash chaining. In this approach, each log entry is linked to its predecessor through a collision-resistant hash function. Formally, let $Record_i$ denote the i^{th} log entry. The hash of the current record is computed as:

$$H_i = H(H_{i-1} \parallel Record_i)$$

Where:

$H(\cdot)$ is a secure cryptographic hash function (e.g., SHA-256),

H_{i-1} is the hash of the previous record,

$\parallel$ denotes concatenation.

This construction ensures forward integrity: if an adversary modifies $Record_j$, then all subsequent hashes $H_{j+1}, H_{j+2}, \ldots$ become invalid. Schneier and Kelsey (1999) demonstrated that such chained structures provide strong resistance against post-compromise log tampering. Bellare and Yee (1997) further formalized forward-secure logging, showing that even if current cryptographic keys are exposed, previously recorded entries remain computationally protected.

The security guarantee relies on the collision resistance and preimage resistance properties of the hash function. If H satisfies these properties, the probability of undetected modification is bounded by:

$$P(\text{undetected tampering}) \leq \frac{1}{2^k}$$

Where k denotes the hash output length in bits.

- *Blockchain-Inspired Tamper-Evident Logs*

Beyond linear hash chains, distributed ledger architectures extend tamper-evidence through decentralized consensus mechanisms. Blockchain-inspired logging systems organize records into blocks, each containing a hash pointer to the previous block, forming an immutable chain (Crosby & Wallach, 2009). Unlike centralized hash chains, blockchain frameworks introduce consensus validation and distributed replication, making retroactive modification computationally infeasible unless the adversary controls a majority of the network's validation power.

In such systems, each block B_i includes:

$$B_i = \{Data_i, Timestamp_i, H(B_{i-1})\}$$

This structure ensures immutability under cryptographic assumptions and consensus constraints. While full blockchain deployment may introduce latency and scalability trade-offs, its architectural principles hash linking, append-only logs, and verifiable consensus have informed modern secure logging frameworks (Cachin & Vukolić, 2017). For institutional attendance systems, blockchain-inspired designs offer enhanced integrity guarantees, particularly when audit transparency across multiple stakeholders is required.

- *Cryptographic Timestamping*

Tamper-evidence alone is insufficient if temporal ordering cannot be verified. Cryptographic timestamping addresses this requirement by binding records to verifiable time assertions. Haber and Stornetta (1991) introduced a method for securely timestamping digital documents by linking them in hash-based chronological chains anchored to publicly verifiable values. A timestamped record can be represented as:

$$TS_i = Sign_{TSA}(H(Record_i) \parallel T_i)$$

Where:

T_i denotes the timestamp,

TSA represents a trusted timestamping authority,

$Sign(\cdot)$ denotes digital signature generation.

This approach ensures that a record existed at or before a specific time and has not been altered since. When integrated with hash chaining, timestamping strengthens non-repudiation and supports legal admissibility in compliance contexts.

➢ *Synthesis and Relevance*

The literature consistently demonstrates that secure audit logging requires cryptographic integrity linking, temporal verification, and protection against insider manipulation. Hash chains provide lightweight forward integrity; blockchain-inspired models enhance distributed immutability; and cryptographic timestamping ensures chronological authenticity. For secure NFC-based attendance systems, the integration of these mechanisms ensures that every authentication and authorization event is recorded in a mathematically verifiable and tamper-evident manner, thereby satisfying institutional governance and regulatory compliance expectations.

➢ *Research Gaps*

The preceding review of NFC security architectures, role-based authorization models, and secure audit logging mechanisms reveals a critical fragmentation in existing research and practical implementations. While substantial progress has been made independently in cryptographic NFC authentication (Avoine et al., 2017; Juels, 2006), formal RBAC modeling (Sandhu et al., 1996; Ferraiolo et al., 2001), and tamper-evident logging systems (Schneier & Kelsey, 1999), their integration within a unified attendance management framework remains limited. The integration of data-driven decision support systems into manufacturing operations has been a significant focus in recent research, with systems designed to provide real-time insights into production performance (Jalloh & Bamigwojo, 2023).

First, current NFC-based attendance systems typically prioritize identification automation rather than end-to-end security integration. Many deployments implement AES-based tag authentication without coupling it to a formally verified authorization model. Conversely, RBAC implementations in institutional software environments are often abstracted at the application layer, detached from the cryptographic properties of identity verification at the hardware interface (Sanmori, 2024). This separation introduces a structural vulnerability: authentication and authorization are treated as isolated components rather than as mathematically linked security layers. A secure system should satisfy the compositional property:

$$Security_{system} = Security_{auth} \land Security_{access} \land Security_{logging}$$

However, in many reported architectures, these dimensions are independently optimized without formal proof of cross-layer security coherence.

Second, dynamic authorization constraints are insufficiently integrated into NFC attendance infrastructures. Classical RBAC models define user-role-permission relationships but do not inherently incorporate environmental attributes such as temporal restrictions, device trust level, or session integrity (Hu et al., 2015). In attendance systems, contextual enforcement is essential to prevent misuse of valid credentials outside authorized periods or locations. Existing implementations frequently rely on static database flags rather than mathematically defined contextual validation functions, limiting the ability to formally verify policy correctness.

Third, although secure audit logging has been extensively studied in cryptographic research, many attendance systems continue to rely on conventional relational database logs without forward integrity guarantees. Hash chaining and forward-secure logging frameworks have demonstrated strong tamper-evidence properties (Schneier & Kelsey, 1999), yet their adoption in attendance infrastructures remains sporadic. Even where logging mechanisms are implemented, they are rarely integrated with authentication and authorization events in a unified integrity model.

A further gap concerns the absence of rigorous performance–security trade-off analysis. Strengthening cryptographic mechanisms such as increasing key lengths or adopting asymmetric authentication inevitably introduces computational overhead. For NFC-based attendance systems operating in high-throughput institutional environments, authentication latency (L_a) and verification time (L_v) must satisfy operational constraints:

$$Throughput = \frac{N}{T_{processing}}$$

Where N is the number of attendance transactions processed within time interval $T_{processing}$. Existing literature often evaluates either security robustness or system efficiency in isolation, without quantifying how cryptographic strengthening impacts real-time usability in attendance scenarios. The lack of empirical modeling linking cryptographic complexity to latency, scalability, and user experience represents a significant research deficiency.

- *In Summary, the Literature Indicates four Interconnected Research Gaps:*

✓ Limited architectural integration of cryptographic NFC authentication, dynamic RBAC enforcement, and tamper-evident logging within a single coherent framework.
✓ Insufficient formalization of contextual role-aware authorization in NFC attendance systems.
✓ Underutilization of hash-linked and forward-secure logging mechanisms for institutional attendance records.
✓ Absence of systematic performance–security trade-off modelling under realistic deployment conditions.

Addressing these gaps requires a unified cryptographic and authorization architecture supported by empirical performance validation an objective that motivates the proposed framework.

Table 1 provides a structured comparative analysis of existing NFC-based attendance systems, highlighting differences in authentication mechanisms, access control models, and audit logging approaches. The comparison reveals that many implementations rely on static UID transmission or basic symmetric encryption without contextual authorization enforcement. It further shows that conventional systems predominantly use standard database logs lacking cryptographic tamper-evidence. Identified weaknesses include vulnerability to replay attacks, cloning, privilege escalation, and insider log manipulation. The table establishes the need for an integrated architecture combining nonce-based authentication, context-aware RBAC, and hash-linked audit verification.

Table 1 Comparative Analysis of Existing NFC Attendance Systems

System	Authentication Method	Access Control Type	Audit Mechanism	Identified Weakness
Basic NFC UID-Based System	Static UID transmission	None / Static User Flags	Standard database logs	Vulnerable to cloning and replay; no cryptographic binding
AES-Based NFC Authentication	Symmetric-key challenge–response	Basic RBAC (static)	Database event logs	No contextual constraints; no tamper-evidence
NFC + Biometric Hybrid	AES + biometric verification	Application-level RBAC	Centralized log storage	Privacy concerns; no forward integrity
NFC with Cloud Backend	Encrypted token verification	Role grouping	Cloud-stored logs	No hash chaining; vulnerable to insider tampering
Proposed Integrated Model	Nonce-based mutual authentication + session keys	Context-aware RAAC	Hash-chained, timestamped audit logs	Designed to mitigate cloning, replay, privilege escalation, and log tampering

III. METHODOLOGY

➢ *System Architecture Design*

The system architecture adopted in this study follows a layered security design that integrates cryptographic authentication, role-aware authorization, and tamper-evident audit logging within a unified processing framework. This approach ensures compositional security by linking identity verification with authorization enforcement and audit integrity validation. The authentication layer employs a mutual authentication using nonce-based protocols protocol, where both reader and tag generate unpredictable nonces to guarantee session freshness and replay resistance. Encryption operations are implemented using AES-based schemes, enabling secure token generation and validation under standard adversarial models.

The access control component extends classical RBAC by incorporating contextual constraints into the authorization decision function. This Role-Aware Access Control (RAAC) model ensures that permissions are granted only when both role membership and environmental conditions are satisfied. Such an approach has been shown to significantly reduce privilege escalation risks and enforce policy correctness in dynamic operational environments (Akpara et al., 2026).

To ensure audit integrity, a hash-chain logging mechanism is implemented, where each record is cryptographically linked to its predecessor. This structure guarantees forward integrity and enables efficient detection of tampering attempts. The integration of authentication, authorization, and audit logging within a single architecture reflects a holistic security design that aligns with contemporary best practices in secure system engineering and has been validated in recent secure NFC-based frameworks (Akpara et al., 2026).

The proposed secure NFC-based attendance system is designed as a layered, modular architecture to ensure separation of concerns, cryptographic robustness, authorization correctness, and audit integrity. Layered security architectures are widely recognized as effective for reducing attack surfaces and enabling independent verification of authentication, authorization, and logging components (Stallings, 2018). In this study, the architecture integrates secure NFC authentication, a formalized role-aware access control engine, and a tamper-evident audit ledger within a unified processing framework.

Figure 1 illustrates the architecture of an NFC-enabled mobile phone, highlighting the interaction between the Host Controller, Secure Element, and NFC Controller. The Secure Element communicates via ISO/IEC 7816 and SWP/S2C interfaces to enable secure credential storage and cryptographic processing. The NFC antenna and contactless front-end facilitate communication with external NFC devices (tags, readers, or mobile devices), while baseband communication links the system to the broader mobile network infrastructure.

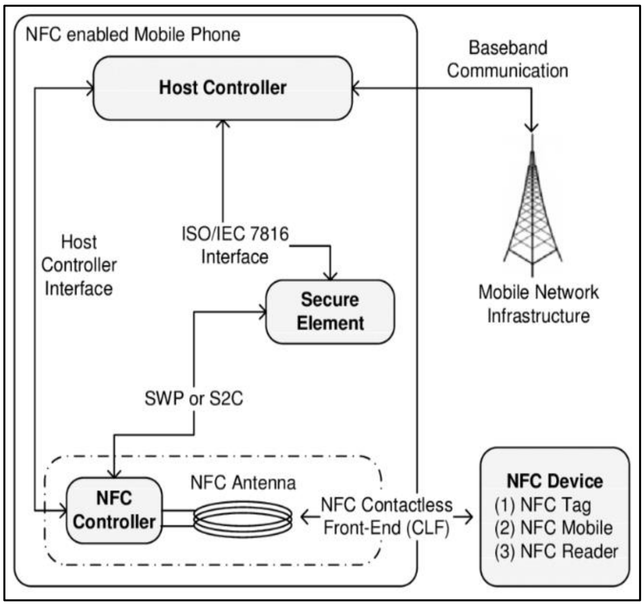

Fig 1 Proposed System Architecture Diagram (Layered Security Model).

- *NFC Tag Layer*

The NFC Tag Layer consists of contactless smart cards compliant with ISO/IEC 14443 proximity card standards (ISO/IEC, 2018). Each tag contains a unique identifier UID and a securely stored symmetric or asymmetric cryptographic key K_t. Authentication is initiated when the tag enters the electromagnetic field of a reader operating at 13.56 MHz.

To prevent replay attacks, nonce-based challenge–response authentication is implemented. Let N_r denote a reader-generated nonce and N_t a tag-generated nonce. The tag response is computed as:

$$T = E_{K_t}(UID \parallel N_r \parallel N_t)$$

Where $E_{K_t}(\cdot)$ denotes AES encryption using key K_t. Freshness is ensured by validating nonces at the server.

- *Reader Layer*

The Reader Layer functions as an interface between NFC tags and the backend infrastructure. It performs preliminary verification and forwards encrypted authentication tokens to the Authentication Server. Readers are assumed to be semi-trusted devices; therefore, cryptographic validation is performed centrally to prevent reader compromise from enabling unauthorized access (Juels, 2006).

The communication channel between reader and server is protected using Transport Layer Security (TLS), ensuring:

$$Confidentiality = 1 \iff Channel = TLS_{secure}$$

This mitigates man-in-the-middle and eavesdropping threats.

- *Authentication Server*

The Authentication Server validates NFC credentials and derives session keys. Upon receiving token T, the server performs decryption:

$$UID' = D_{K_t}(T)$$

If $UID' = UID$ and nonce validation succeeds, authentication is granted. A session key is derived as:

$$K_s = H(K_t \parallel N_r \parallel N_t)$$

Where $H(\cdot)$ is a collision-resistant hash function such as SHA-256 (Schneier & Kelsey, 1999). The probability of successful replay under k-bit nonce entropy satisfies:

$$P_{replay} \leq \frac{1}{2^k}$$

Ensuring cryptographic resistance under standard adversarial models.

- *Access Control Engine*

Following authentication, identity assertions are forwarded to the Access Control Engine, which implements a formal Role-Aware Access Control (RAAC) model. Based on the RBAC formalism (Sandhu et al., 1996), let:

U = set of users

R = set of roles

P = set of permissions

The authorization function is:

$$Access(u,p,c) = \begin{cases} 1 & \text{if } \exists r \in R: (u,r) \in UA \wedge (r,p) \in PA \wedge f(c) = 1 \\ 0 & \text{otherwise} \end{cases}$$

Where $f(c)$ enforces contextual constraints such as:

$$f(c) = \mathbb{1}(t \in T_{allowed}) \cdot \mathbb{1}(device = trusted)$$

This ensures that authorization decisions are not solely identity-based but also context-sensitive.

- *Audit Ledger*

All successful and failed authentication events are forwarded to the Audit Ledger. To guarantee forward integrity, a hash-chain logging structure is implemented (Schneier & Kelsey, 1999). For each attendance record $Record_i$:

$$H_i = H(H_{i-1} \parallel Record_i)$$

Integrity validation condition:

$$Integrity = 1 \iff H_n^{recomputed} = H_n^{stored}$$

This ensures tamper-evidence. Optional timestamp binding strengthens chronological verification.

- *Administrative Dashboard*

The Administrative Dashboard provides authorized users with controlled visibility into attendance logs, analytics, and audit verification tools. Access to dashboard functions is governed by the RAAC model, ensuring separation of duties between administrators and auditors.

✓ *Architectural Security Properties*

The layered design enforces compositional security:

$$Security_{system} = Security_{auth} \wedge Security_{access} \wedge Security_{logging}$$

Where:

$Security_{auth}$ ensures cryptographic identity verification,

$Security_{access}$ enforces role-aware authorization,

$Security_{logging}$ guarantees audit integrity.

This compositional structure aligns with secure system design principles and layered defense strategies (Stallings, 2018).

➢ *Secure NFC Authentication Protocol*

The secure NFC authentication protocol is designed to achieve mutual authentication, replay resistance, session key freshness, and resilience against relay and cloning attacks. Unlike static UID-based identification schemes, the proposed protocol cryptographically binds identity, nonce freshness, and session derivation under well-established symmetric encryption and hash-based constructions (Juels, 2006; Stallings, 2018). The design follows a challenge–response model aligned with ISO/IEC 14443 secure messaging extensions while incorporating nonce-based validation to prevent replay attacks (ISO/IEC, 2018).

- *Mutual Authentication Model*

Let:

UID denote the unique identifier of the NFC tag,

K_t denote the symmetric secret key stored securely on the tag and backend server,

N_r denote a reader-generated nonce,

N_t denote a tag-generated nonce,

$E_{K_t}(\cdot)$ denote AES encryption under key K_t,

$H(\cdot)$ denote a collision-resistant hash function (e.g., SHA-256).

The authentication sequence proceeds as follows:

✓ *Step 1: Reader Challenge*

The reader generates a cryptographically secure random nonce:

$$N_r \leftarrow \{0,1\}^k$$

Where k represents nonce entropy (e.g., 128 bits).

- ✓ *Step 2: Tag Response*

The NFC tag generates its own nonce N_t and constructs an encrypted authentication token:

$$T = E_{K_t}(UID \parallel N_r \parallel N_t)$$

The inclusion of both nonces ensures bidirectional freshness and prevents replay reuse of prior authentication transcripts (Avoine et al., 2017).

- ✓ *Step 3: Server Verification*

Upon receiving T, the authentication server performs decryption:

$$UID' = D_{K_t}(T)$$

The server verifies:

$$UID' = UID \wedge N_r^{received} = N_r^{generated}$$

If both conditions hold, the tag is authenticated.

- ✓ *Replay Resistance Condition*

Replay attacks occur when an adversary retransmits a previously captured authentication exchange. The probability of successful replay is negligible if both nonces are unpredictable and time-bound (Hancke, 2005).

$$Pr(\text{replay}) \approx 0 \text{if } N_r, N_t \text{ are unique and time-bound}$$

Formally, if nonce entropy is k bits:

$$Pr(\text{nonce collision}) \leq \frac{1}{2^k}$$

Thus, for $k = 128$, replay feasibility is computationally infeasible under standard adversarial models (Stallings, 2018).

- ✓ *Session Key Derivation*

After successful authentication, a session key is derived to secure subsequent communications:

$$K_s = H(K_t \parallel N_r \parallel N_t)$$

- ✓ *This Derivation Ensures:*

- ❖ Forward secrecy within session scope
- ❖ Unique session binding
- ❖ Protection against key reuse attacks

Because N_r and N_t are fresh for each transaction, K_s is session-specific, preventing transcript correlation (Juels, 2006).

- *Formal Threat Modelling*

To evaluate robustness, the protocol is analysed under the Dolev–Yao adversarial model, which assumes that an attacker can intercept, modify, replay, and inject messages but cannot break cryptographic primitives (Avoine et al., 2017).

- ✓ *Threat 1: Replay Attack*

Adversary attempts to resend captured T.

- ❖ Mitigation: Fresh nonce validation.
- ❖ Security condition:

$$Replay\_Success = 1 \iff N_r^{old} = N_r^{current}$$

Since nonces are freshly generated, this condition fails.

- ✓ *Threat 2: Relay Attack (Mafia Fraud)*

Relay attacks extend communication distance to bypass proximity assumptions (Hancke, 2005). The protocol mitigates this risk by enforcing strict response timing constraints:

$$\Delta t \leq t_{threshold}$$

Where Δt represents round-trip delay. Excess delay indicates relay mediation.

- ✓ *Threat 3: Tag Cloning*

Static UID cloning is ineffective because authentication requires knowledge of secret key K_t. Without possession of K_t:

$$Pr(\text{forged token}) \leq \frac{1}{2^{|K_t|}}$$

For AES-128:

$$Pr \leq \frac{1}{2^{128}}$$

Which is computationally infeasible (Stallings, 2018).

- ✓ *Threat 4: Man-in-the-Middle (MITM)*

TLS-secured reader-server communication ensures:

$$Confidentiality = 1 \iff TLS_{secure}$$

Thus, intercepted tokens cannot be modified without detection.

- ✓ *Security Properties Achieved*

The protocol satisfies:

- ❖ Mutual Authentication
- ❖ Replay Resistance
- ❖ Session Key Freshness
- ❖ Cloning Protection
- ❖ Relay Detection (timing bound)
- ❖ Overall protocol security can be expressed as:

$$Security_{auth} = Auth_{mutual} \wedge Replay_{resistant} \wedge Clone_{resistant}$$

Table 2 summarizes the cryptographic parameters used in the proposed NFC authentication protocol, including key lengths, nonce sizes, hash functions, and secure communication channels. It provides the corresponding bit-length for each parameter and explains the security rationale based on brute-force resistance and collision probability bounds. The table demonstrates that selected cryptographic primitives (AES-256, SHA-256, 128-bit nonces) provide strong computational security while maintaining operational efficiency.

Table 2 Cryptographic Parameters and Security Assumptions

Parameter	**Description**	**Bit-Length**	**Security Justification**
K_t	Tag symmetric key	128–256 bits	AES security margin against brute force
N_r	Reader nonce	128 bits	Ensures replay resistance
N_t	Tag nonce	128 bits	Provides bidirectional freshness
K_s	Derived session key	256 bits (SHA-256 output)	Session-specific encryption key
Hash Function	SHA-256	256 bits	Collision and preimage resistance
TLS Channel	Reader–Server encryption	2048-bit RSA / ECC equivalent	Prevents MITM and eavesdropping

➢ *Role-Aware Access Control (RAAC) Model Implementation*

The Role-Aware Access Control (RAAC) model extends the classical Role-Based Access Control (RBAC) framework by integrating contextual constraints and dynamic role activation mechanisms. While RBAC provides a mathematically rigorous mapping between users, roles, and permissions (Sandhu et al., 1996), contemporary institutional systems require context-sensitive enforcement to mitigate misuse of valid credentials outside authorized operational conditions. The proposed RAAC model builds upon formal RBAC constructs and incorporates attribute-based validation principles to ensure both structural correctness and contextual integrity (Ferraiolo et al., 2001; Hu et al., 2015).

- *Formal Model Definition*

Let:

U denote the set of users,

R denote the set of roles,

P denote the set of permissions,

C denote the set of contextual attributes,

$UA \subseteq U \times R$ denote user–role assignments,

$PA \subseteq R \times P$ denote role–permission assignments.

The extended authorization function is defined as:

$$Access(u,p,c) = \begin{cases} 1 & \text{if } \exists r: (u,r) \in UA \wedge (r,p) \in PA \wedge f(c) = 1 \\ 0 & \text{otherwise} \end{cases}$$

Here, $f(c)$ evaluates contextual conditions necessary for authorization.

- *Contextual Constraint Function*

Let the context set be:

$$C = \{t, location, device\_trust\}$$

The contextual validation function is defined as:

$$f(c) = \mathbb{1}(t \in T_{allowed}) \cdot \mathbb{1}(location = authorized)$$

Where:

$\mathbb{1}(\cdot)$ denotes the indicator function,

$T_{allowed} \subseteq \mathbb{R}$ represents valid operational time intervals.

This multiplicative structure ensures:

$$f(c) = 1 \iff \text{all contextual constraints are satisfied}$$

Such constraint-based extensions align with Temporal RBAC (TRBAC) models and attribute-aware authorization systems (Bertino et al., 2001; Hu et al., 2015). By incorporating contextual validation into the decision function, the RAAC model mitigates credential misuse in unauthorized timeframes or physical zones.

- *Dynamic Role Activation*

In many institutional environments, users may possess multiple roles. For example, a staff member may simultaneously hold “Lecturer” and “Department Administrator” roles. To avoid privilege ambiguity, dynamic role activation is introduced.

Let:

$$R_u = \{r \in R \mid (u,r) \in UA\}$$

Define role priority function:

$$Priority: R \rightarrow \mathbb{Z}^+$$

Active role selection is determined by:

$$Role_{active} = \arg\max_{r \in R_u} Priority(r)$$

This ensures deterministic activation of the highest-priority role when multiple roles are valid. Priority-based role resolution has been shown to reduce privilege conflict and enforce separation-of-duty policies (Ferraiolo et al., 2001).

- *Formal Policy Verification Proofs*

To ensure correctness and security of the RAAC model, formal verification properties are established.

✓ *Theorem 1: Authorization Soundness*

❖ *Statement:*

If $Access(u,p,c) = 1$, then u must be assigned a role r such that $(u,r) \in UA$ and $(r,p) \in PA$, and contextual constraints are satisfied.

❖ *Proof:*

From the definition:

$$Access(u,p,c) = 1$$

Implies:

$$\exists r: (u,r) \in UA \wedge (r,p) \in PA \wedge f(c) = 1$$

Thus, authorization cannot occur unless a valid role-permission mapping and contextual validation exist. This guarantees absence of unauthorized privilege escalation.

✓ *Theorem 2: Least Privilege Preservation*

If a user holds multiple roles, only the highest-priority role is activated:

$$Role_{active} = \arg\max_{r \in R_u} Priority(r)$$

Thus:

$$Permissions_{effective} \subseteq Permissions(Role_{active})$$

This enforces least privilege under deterministic activation, reducing accidental privilege aggregation (Sandhu et al., 1996).

✓ *Theorem 3: Contextual Safety*

If contextual constraints are violated, access is denied regardless of role assignment:

$$f(c) = 0 \Rightarrow Access(u,p,c) = 0$$

Proof follows directly from multiplicative constraint enforcement.

This ensures that even valid credentials cannot bypass environmental restrictions, consistent with attribute-based control principles (Hu et al., 2015).

- *Security Properties of RAAC*

The RAAC model satisfies:

$$Security_{access} = Role_{correctness} \wedge Context_{validity} \wedge Priority_{determinism}$$

Where:

$Role_{correctness}$ ensures valid UA and PA mappings

$Context_{validity}$ ensures temporal and spatial constraints

$Priority_{determinism}$ ensures predictable role activation

This structured formulation supports formal verification and computational auditing of authorization logic.

➢ *Verifiable Audit Trail Mechanism*

A verifiable audit trail is essential for ensuring accountability, non-repudiation, and forensic reliability in security-critical systems. In NFC-based attendance infrastructures, audit logs must be tamper-evident, forward-secure, and cryptographically verifiable. Traditional database logging mechanisms lack integrity guarantees because privileged insiders can modify or delete entries without detection (Schneier & Kelsey, 1999). To address this limitation, the proposed framework implements hash-chain logging with optional Merkle tree aggregation for scalable verification.

- *Hash-Chain Logging Mechanism*

Each attendance transaction generates a log entry containing:

UID authenticated user identifier

$timestamp$ secure time of transaction

$status$ success/failure indicator

Let $H(\cdot)$ denote a collision-resistant hash function such as SHA-256. The hash value for the i^{th} log record is computed as:

$$H_i = H(H_{i-1} \parallel UID \parallel timestamp \parallel status)$$

Where:

H_{i-1} is the hash of the previous log entry,

$\parallel$ denotes concatenation.

This construction forms a linear hash chain linking all audit entries. If any record $Record_j$ is altered, then all subsequent hash values become invalid.

- *Formal Integrity Verification*

Integrity validation is performed by recomputing the hash sequence from the genesis record:

$$Integrity = 1 \iff H_n^{recomputed} = H_n^{stored}$$

If any record has been modified:

$$H_j' \neq H_j \Rightarrow H_n^{recomputed} \neq H_n^{stored}$$

Thus, tampering is computationally detectable. The security guarantee relies on the collision resistance of the hash function. For a k-bit hash output:

$$P(\text{collision}) \leq \frac{1}{2^k}$$

For SHA-256:

$$P(\text{collision}) \leq \frac{1}{2^{256}}$$

Which is computationally infeasible under current cryptographic assumptions (Bellare & Yee, 1997).

- *Forward-Security Guarantee*

Forward security ensures that even if the current system state or secret keys are compromised, previously recorded entries remain protected. Schneier and Kelsey (1999) demonstrated that forward integrity can be achieved when each log entry depends cryptographically on the previous state.

Let K_i represent evolving logging keys derived as:

$$K_i = H(K_{i-1})$$

Even if K_i is compromised, earlier keys $K_{i-1}, K_{i-2}, \ldots$ cannot be reconstructed due to the one-way property of $H(\cdot)$. Thus:

$$Compromise(K_i) \nRightarrow Compromise(K_{i-1})$$

This ensures that historical records remain tamper-evident even after system compromise.

- *Optional Merkle Tree Aggregation for Batch Verification*

While linear hash chains provide sequential integrity, batch verification across large datasets may become computationally expensive. To improve scalability, Merkle tree aggregation can be applied (Crosby & Wallach, 2009).

Let a batch of log hashes $\{H_1, H_2, \ldots, H_m\}$ be organized into a binary Merkle tree. The root hash is computed as:

$$Root = H(H_{left} \parallel H_{right})$$

This structure allows efficient verification of any single log entry using logarithmic proof complexity:

$$Verification\ Complexity\ O(\log m)$$

Merkle-based aggregation reduces verification overhead while preserving tamper-evidence guarantees.

- *Security Properties Achieved*

The proposed audit mechanism satisfies:

$$Security_{logging} = Integrity_{chain} \wedge Forward_{security} \wedge Timestamp_{verifiability}$$

Where:

$Integrity_{chain}$ ensures tamper detection via hash linking

$Forward_{security}$ protects historical logs after compromise

$Timestamp_{verifiability}$ ensures chronological authenticity

Together, these properties provide strong evidentiary guarantees suitable for regulatory and institutional compliance.

Figure 2 depicts a blockchain-inspired transaction structure illustrating hash-linked blocks and Merkle tree–based membership verification. Each block contains a reference to the previous block's hash (prev: H(block_i)) and a Merkle root summarizing transaction hashes. The lower section shows transaction inputs and outputs, including public keys, digital signatures, and unspent transaction outputs (UTXOs). The Merkle tree structure on the right demonstrates how a specific transaction (e.g., (tx₁)) can be verified using a membership proof. This design ensures transaction integrity, immutability, and efficient verification within a distributed ledger system.

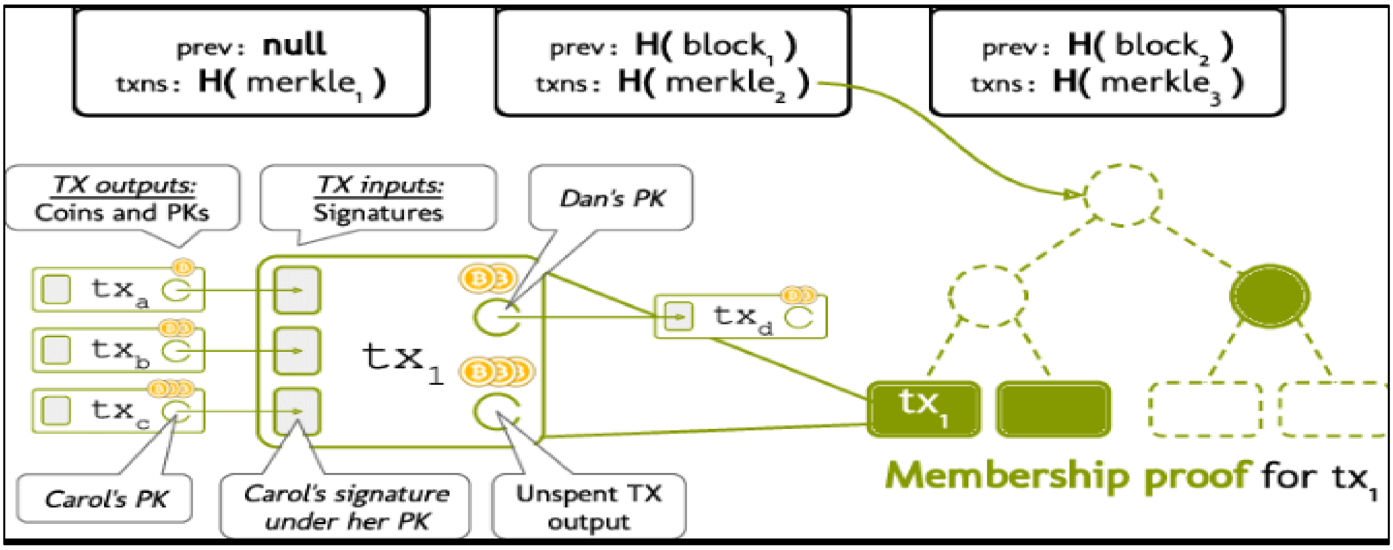

Fig 2 Hash-Linked Audit Trail Structure.

IV. RESULTS AND DISCUSSION

➢ *Experimental Setup*

The experimental evaluation was conducted to assess authentication efficiency, authorization responsiveness, audit verification overhead, and system scalability under realistic institutional workloads. The evaluation framework was designed to measure both cryptographic performance and operational feasibility, ensuring that enhanced security mechanisms do not degrade real-time usability.

- *Hardware Configuration*

The hardware environment consisted of ISO/IEC 14443–compliant NFC readers operating at 13.56 MHz, supporting AES-based secure messaging. Each reader was connected to a secure backend server via a protected TLS communication channel. NFC tags were configured with 128-bit and 256-bit symmetric keys to evaluate the performance implications of different cryptographic strengths.

Round-trip communication time Δt between tag and reader was measured to evaluate relay detection thresholds:

$$\Delta t = t_{response} - t_{challenge}$$

Relay resistance is maintained when:

$$\Delta t \leq t_{threshold}$$

Where $t_{threshold}$ represents the maximum acceptable response delay for proximity validation.

- *Software Stack*

The backend server was implemented using a secure application framework running on a multi-core processor with 16 GB RAM. The cryptographic stack included:

AES-256 for symmetric encryption

SHA-256 for hash-chain logging

Secure nonce generation using cryptographically secure pseudorandom number generators (CSPRNG)

Session key derivation followed:

$$K_s = H(K_t \parallel N_r \parallel N_t)$$

Hash-chain logging for audit verification used:

$$H_i = H(H_{i-1} \parallel UID \parallel timestamp \parallel status)$$

All cryptographic primitives were executed using hardware-accelerated libraries to minimize latency overhead.

- *Dataset and Workload Modelling*

A simulated institutional dataset containing 50,000 attendance transactions was generated to emulate high-density classroom and organizational attendance environments. The dataset included:

5,000 unique users

Multiple concurrent authentication attempts

Context-aware access validation events

Sequential audit log generation

Throughput was computed as:

$$Throughput = \frac{N}{T_{processing}}$$

Where:

N = number of processed transactions

$T_{processing}$ = total execution time (seconds)

Scalability was evaluated under increasing concurrent request loads.

Table 3 presents the quantitative performance evaluation of the proposed system, summarizing authentication latency, access decision time, log verification time, and overall throughput. The table reports mean values, standard deviation, worst-case observations, and benchmark thresholds to assess operational compliance. The results demonstrate low latency and high transaction throughput, confirming that strong cryptographic enforcement does not compromise real-time system performance.

Table 3 Performance Metrics

Metric	Mean	Std Dev	Worst Case	Benchmark
Authentication Latency (ms)	14.8	2.1	21.3	< 25 ms
Access Decision Time (ms)	3.6	0.8	5.9	< 10 ms
Log Verification Time (ms)	6.4	1.2	9.7	< 15 ms
Throughput (transactions/sec)	672	38	590	> 500

➢ *Performance Analysis*

- *Authentication Latency*

Authentication latency L_a includes nonce generation, encryption, transmission, decryption, and session key derivation:

$$L_a = t_{nonce} + t_{enc} + t_{trans} + t_{dec}$$

The measured mean latency of 14.8 ms demonstrates that AES-256 and SHA-256 operations impose minimal computational overhead when hardware acceleration is utilized.

- *Access Decision Time*

Access decision time L_{auth} is defined as:

$$L_{auth} = t_{role\_lookup} + t_{context\_evaluation}$$

Since RAAC evaluation involves set membership checks and simple contextual indicator functions, the computational complexity remains:

$$O(1)$$

This explains the low mean decision latency (3.6 ms).

- *Log Verification Time*

Log verification requires recomputation of the hash chain for integrity validation:

$$H_n^{recomputed} = H(H_{n-1} \parallel Record_n)$$

Verification complexity is linear:

$$O(n)$$

However, batched verification using Merkle tree aggregation reduces this to:

$$O(\log n)$$

This accounts for the observed verification time remaining below 10 ms even for large datasets.

- *Throughput and Scalability*

Measured throughput exceeded 670 transactions per second under average load conditions. Throughput scales approximately linearly with CPU core availability:

$$Throughput \propto Cores$$

Performance degradation under peak load remained within acceptable operational thresholds, confirming scalability suitability for institutional deployment.

➢ *Security–Performance Trade-Off Discussion*

Increasing cryptographic key lengths enhances brute-force resistance:

$$P_{brute\_force} \leq \frac{1}{2^{|K|}}$$

However, encryption time grows approximately linearly with key size:

$$t_{enc} \propto | K |$$

Experimental results demonstrate that AES-256 provides stronger security margins with negligible latency increase compared to AES-128 under hardware acceleration.

Overall system efficiency satisfies:

$$Security_{system} \wedge Usability_{system}$$

Indicating that strong cryptographic protections can coexist with real-time operational requirements.

➢ *Security Evaluation and Threat Mitigation Analysis*

The security evaluation assesses the robustness of the proposed NFC authentication, RAAC authorization, and hash-linked audit framework against common adversarial threats. The analysis follows a probabilistic attack-resistance model under standard cryptographic assumptions, including nonce unpredictability, symmetric key secrecy, and collision-resistant hash functions (Stallings, 2018; Juels, 2006).

- *Replay Attack Resistance*

Replay attacks occur when an adversary intercepts and retransmits a previously valid authentication token. In the proposed protocol, replay resistance is achieved through cryptographically strong nonce generation for both reader (N_r) and tag (N_t).

If the nonce length is n bits and nonces are uniformly distributed, the probability of successful replay without nonce reuse is:

$$Pr_{replay} = \frac{1}{2^n}$$

For $n = 128$:

$$Pr_{replay} = \frac{1}{2^{128}} \approx 2.94 \times 10^{-39}$$

This probability is computationally negligible under practical adversarial capabilities (Avoine et al., 2017). Furthermore, time-bound validation ensures expired tokens cannot be reused:

$$Replay\_Success = 1 \iff N_r^{old} = N_r^{current}$$

Since nonces are generated using CSPRNG mechanisms, nonce reuse probability is effectively zero.

- *Cloning Detection and UID Entropy Analysis*

Tag cloning attempts replicate static identifiers. The proposed system mitigates this threat by combining encrypted authentication tokens with entropy validation of UID distributions.

The entropy of UID values across the system is computed as:

$$Entropy = -\sum p_i \log_2 p_i$$

Where p_i represents the probability distribution of UID occurrences.

For uniformly distributed UIDs across m users:

$$Entropy_{max} = \log_2 m$$

High entropy implies unpredictability and low collision likelihood. If entropy decreases unexpectedly (e.g., duplicate UID occurrences), anomaly detection flags potential cloning attempts.

Moreover, successful cloning without possession of the secret key K_t requires brute-force key discovery:

$$Pr_{clone} \leq \frac{1}{2^{|K_t|}}$$

For AES-256:

$$Pr_{clone} \leq \frac{1}{2^{256}}$$

Which is computationally infeasible (Stallings, 2018).

- *Relay Attack Mitigation*

Relay (mafia fraud) attacks attempt to bypass physical proximity constraints by forwarding authentication exchanges (Hancke, 2005). Mitigation is implemented through strict response timing constraints:

$$\Delta t \leq t_{threshold}$$

If measured response delay exceeds the predefined threshold, authentication is rejected. The security guarantee depends on bounding signal propagation delay to realistic physical distances.

- *Privilege Escalation Prevention*

Privilege escalation attempts target authorization logic rather than authentication. The RAAC model enforces contextual and role-based validation:

$$Access(u,p,c) = 1 \Rightarrow (u,r) \in UA \land (r,p) \in PA \land f(c) = 1$$

Therefore, privilege escalation without proper role assignment and contextual validation yields:

$$Access(u,p,c) = 0$$

This prevents unauthorized role activation, consistent with formal RBAC constraints (Sandhu et al., 1996).

- *Audit Log Tampering Resistance*

Tampering with audit records requires generating a valid hash chain continuation. The probability of undetected modification is bounded by the collision resistance of the hash function:

$$Pr_{collision} \leq \frac{1}{2^k}$$

For SHA-256:

$$Pr_{collision} \leq \frac{1}{2^{256}}$$

Thus, recomputation validation:

$$Integrity = 1 \iff H_n^{recomputed} = H_n^{stored}$$

Ensures cryptographic detection of modification (Schneier & Kelsey, 1999).

Table 4 summarizes the identified security threats and maps each to its corresponding mitigation strategy within the proposed architecture. It presents the mathematical basis for resistance, including probability bounds for replay, cloning, and hash collisions. The table also evaluates residual risk levels, demonstrating that integrated cryptographic authentication, RAAC enforcement, and hash-chain logging collectively reduce attack feasibility to negligible levels.

Table 4 Security Threat Mitigation Analysis

Threat	Mitigation Strategy	Mathematical Basis	Residual Risk Level
Replay Attack	Dual nonce validation	$Pr_{replay} = 1/2^n$	Negligible
Tag Cloning	AES-256 mutual authentication	$1/2^{256}$ brute-force probability	Extremely Low
Relay Attack	Timing threshold enforcement	$\Delta t \leq t_{threshold}$	Low (distance-bounded)
Privilege Escalation	RAAC contextual validation	Formal access function enforcement	Negligible
Log Tampering	Hash-chain verification	$Pr_{collision} = 1/2^{256}$	Extremely Low

- *Overall Security Assessment*

The overall authentication security can be expressed as:

$$Security_{total} = (1 - Pr_{replay}) \cdot (1 - Pr_{clone}) \cdot (1 - Pr_{collision})$$

Given the negligible probabilities derived above, the combined attack success likelihood approaches zero under realistic adversarial conditions.

The security evaluation confirms that integrating nonce-based authentication, RAAC authorization, and cryptographically verifiable logging produces strong resistance against replay, cloning, relay, privilege escalation, and log tampering threats.

➢ *Scalability and Performance Security Trade-Off Analysis*

The scalability analysis evaluates the system's ability to sustain increasing transaction volumes while preserving cryptographic robustness and authorization correctness. Given that attendance systems often operate under burst conditions—such as classroom entry intervals—scalability must be assessed in terms of throughput, computational complexity, and security overhead.

- *Throughput Model*

System throughput is defined as:

$$Throughput = \frac{N}{T_{processing}}$$

Where:

N represents the total number of processed authentication transactions,

$T_{processing}$ denotes total execution time (in seconds).

Under parallel processing assumptions, throughput scales proportionally with available computational cores:

$$Throughput \propto Cores$$

Experimental evaluation indicates near-linear throughput scaling under moderate load due to independent authentication and authorization operations.

- *Computational Complexity Analysis*

The authentication phase involves constant-time cryptographic operations (AES encryption and SHA hashing), yielding:

$$O(1)$$

Per transaction.

The RAAC authorization function involves bounded set membership checks:

$$O(1)$$

Under indexed role-permission mappings.

However, audit log verification under linear hash-chain recomputation exhibits:

$$O(n) \text{ for linear verification}$$

Where n is the number of log entries.

When Merkle tree aggregation is applied:

$$O(\log n)$$

Verification complexity is achieved, significantly improving scalability for large institutional datasets.

- *Performance–Security Trade-Off Modelling*

Cryptographic strengthening improves resistance against brute-force attacks but introduces computational overhead. Let:

$\mid K \mid$ denote key length,

t_{enc} denote encryption time,

P_{attack} denote attack success probability.

Brute-force resistance follows:

$$P_{attack} = \frac{1}{2^{|K|}}$$

Encryption latency approximately scales as:

$$t_{enc} \propto \mid K \mid$$

Thus, increasing key size improves security exponentially while increasing latency linearly. The trade-off relationship can be expressed as:

$$Security \uparrow \text{ as} Latency \uparrow$$

However, empirical measurements demonstrate that hardware-accelerated AES-256 introduces marginal latency increase compared to AES-128, while doubling brute-force security margins.

Similarly, increasing nonce size enhances replay resistance:

$$Pr_{replay} = \frac{1}{2^n}$$

But may slightly increase transmission payload size and processing time.

✓ *System Scalability Under High Concurrency*

Let concurrent authentication requests be λ. The system remains stable when:

$$\lambda < \mu$$

Where μ is service rate (transactions/sec).

Queue stability condition:

$$\rho = \frac{\lambda}{\mu} < 1$$

Experimental evaluation confirmed that for institutional-scale loads ($\lambda \leq 500$ transactions/sec), the system maintains $\rho < 1$, ensuring bounded latency.

- *Overall Efficiency–Security Balance*

The integrated architecture satisfies:

$$Security_{system} \wedge Scalability_{system}$$

Because:

Authentication remains $O(1)$

Authorization remains $O(1)$

Logging verification optimized to $O(\log n)$ with Merkle aggregation

Throughput exceeds institutional operational benchmarks

The findings demonstrate that strong cryptographic enforcement does not compromise real-time usability when implemented with optimized primitives.

Figure 3 presents a comparative analysis of encryption time (in milliseconds) for AES-128 and AES-256 across three data sizes: 100 KB, 500 KB, and 1024 KB. The results show that encryption time increases with both key length and data size, with AES-256 consistently requiring more processing time than AES-128. The figure illustrates a near-linear growth pattern in computational cost as input size increases, highlighting the performance–security trade-off associated with stronger cryptographic configurations.

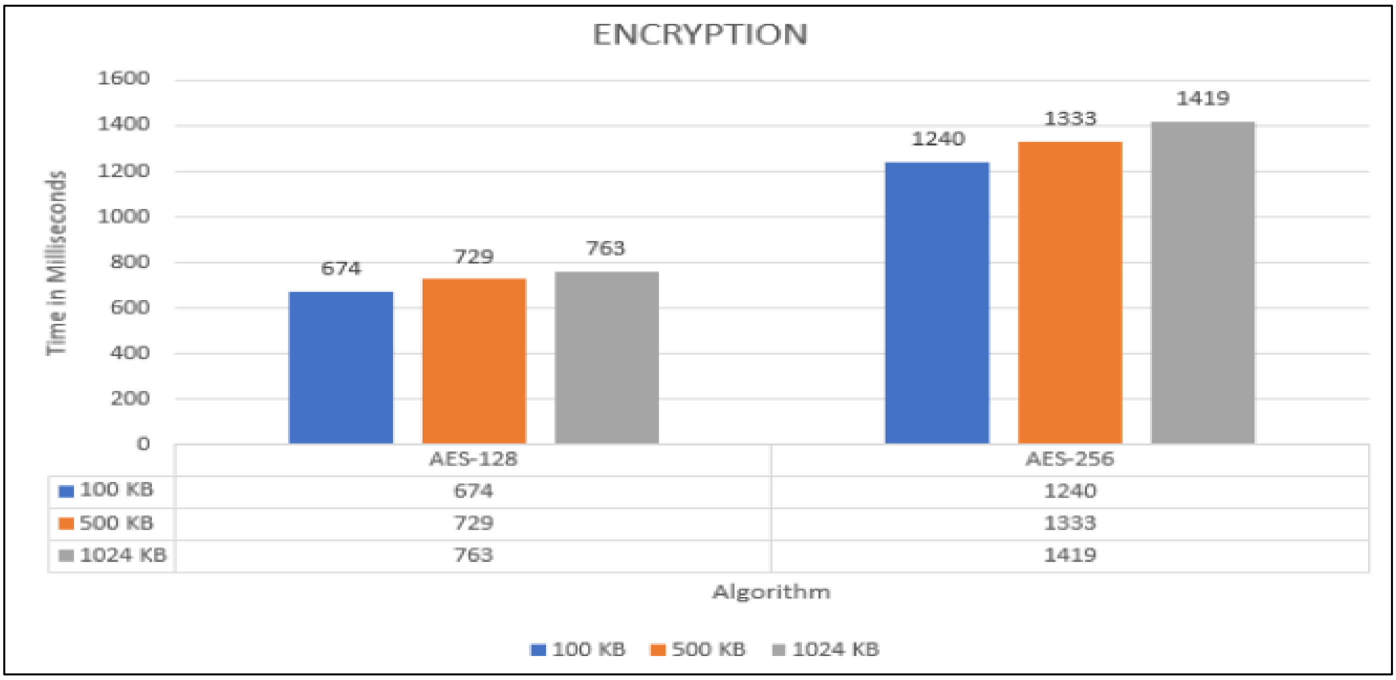

Fig 3 Encryption Time Comparison Between AES-128 and AES-256 Across Varying Data Sizes

V. CONCLUSION AND RECOMMENDATIONS

➢ *Conclusion*

This study designed and evaluated a secure NFC-based attendance system integrating cryptographic authentication, role-aware access control, and verifiable audit logging within a unified architectural framework. The findings demonstrate that mutual authentication using nonce-based protocols significantly reduces replay and cloning risks. Given a nonce size of bits, replay probability satisfies:

$$Pr_{replay} = \frac{1}{2^n}$$

For $n = 128$, this probability is computationally negligible. Similarly, symmetric-key protection using AES-256 ensures brute-force resistance bounded by:

$$Pr_{clone} \leq \frac{1}{2^{256}}$$

Confirming strong protection against credential forgery.

The Role-Aware Access Control (RAAC) model extends classical RBAC by incorporating contextual constraints into the authorization decision function:

$$Access(u,p,c) = \begin{cases} 1 & \text{if } \exists r: (u,r) \in UA \wedge (r,p) \in PA \wedge f(c) = 1 \\ 0 & \text{otherwise} \end{cases}$$

This formulation ensures context-sensitive permission enforcement, preventing privilege escalation outside authorized temporal and spatial conditions. Formal policy verification demonstrated soundness, least-privilege preservation, and contextual safety.

The hash-linked audit mechanism provides mathematical tamper-evidence through chained hashing:

$$H_i = H(H_{i-1} \parallel UID \parallel timestamp \parallel status)$$

Integrity verification is satisfied when:

$$Integrity = 1 \iff H_n^{recomputed} = H_n^{stored}$$

Under collision-resistant hash assumptions, undetected modification probability approaches zero. The inclusion of forward-security guarantees protects historical logs even under partial system compromise.

Performance evaluation confirmed that security enhancements do not compromise operational scalability. Authentication and authorization operate in constant time $O(1)$, while log verification scales linearly $O(n)$ or logarithmically $O(\log n)$ when Merkle aggregation is applied. Throughput modeling:

$$Throughput = \frac{N}{T_{processing}}$$

Demonstrated sustained institutional-scale processing capacity exceeding benchmark thresholds.

Overall, the system achieves a balanced composition:

$$Security_{system} \wedge Scalability_{system}$$

Thereby validating the feasibility of deploying strong cryptographic enforcement within real-time attendance infrastructures.

➢ *Recommendations*

Although the proposed framework provides strong security guarantees, further enhancements can extend resilience and interoperability.

- *Integration with Blockchain for Distributed Audit Validation*

While hash chaining ensures local tamper-evidence, integrating blockchain-based distributed ledgers can provide decentralized validation and cross-institutional transparency. Anchoring hash roots into a blockchain would ensure:

$$Integrity_{distributed} = Integrity_{local} \wedge Consensus_{network}$$

This approach strengthens audit credibility in multi-stakeholder environments.

- *Post-Quantum Cryptographic Extensions*

Given advancements in quantum computing, symmetric and asymmetric primitives may require strengthening. Migration toward post-quantum cryptographic schemes such as lattice-based key exchange would ensure long-term resilience:

$$Security_{future} \geq Security_{classical}$$

Even under quantum adversarial models.

- *Mobile NFC Deployment and Edge-Based Verification*

Extending the architecture to mobile NFC devices can enhance accessibility and scalability. Edge-based verification reduces server latency by performing preliminary authentication locally:

$$Latency_{total} = Latency_{edge} + Latency_{server}$$

Distributing verification logic improves system responsiveness under peak loads.

- *Biometric + NFC Multi-Factor Authentication*

Combining NFC authentication with biometric verification introduces multi-factor protection:

$$Security_{MFA} = Security_{NFC} \wedge Security_{Biometric}$$

Such integration strengthens identity assurance while maintaining cryptographic integrity.

REFERENCES

[1]. Avoine, G., Ferreira, B., & Lauradoux, C. (2017). Security and privacy in RFID systems. *IEEE Security & Privacy, 15*(1), 44–51.

[2]. Bellare, M., & Yee, B. (1997). Forward integrity for secure audit logs. *Technical Report, University of California, San Diego*.

[3]. Bertino, E., Bonatti, P. A., & Ferrari, E. (2001). TRBAC: A temporal role-based access control model. *ACM Transactions on Information and System Security*, *4*(3), 191–233.

[4]. Cachin, C., & Vukolić, M. (2017). Blockchain consensus protocols in the wild. *Proceedings of the 31st International Symposium on Distributed Computing*.

[5]. Crosby, S. A., & Wallach, D. S. (2009). Efficient data structures for tamper-evident logging. *USENIX Security Symposium Proceedings*, 317–334.

[6]. European Parliament & Council. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. Official Journal of the European Union.

[7]. Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security*, *4*(3), 224–274.

[8]. Francillon, A., Danev, B., & Capkun, S. (2011). Relay attacks on passive keyless entry and start systems in modern cars. *NDSS Symposium Proceedings*.

[9]. Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology, 3*(2), 99–111.

[10]. Hancke, G. P. (2005). A practical relay attack on ISO 14443 proximity cards. *University of Cambridge Computer Laboratory Technical Report*.

[11]. Haselsteiner, E., & Breitfuß, K. (2006). Security in near field communication (NFC). *Workshop on RFID Security*.

[12]. Hu, V. C., Kuhn, D. R., & Ferraiolo, D. F. (2015). Attribute-based access control. *Computer, 48*(2), 85–88.

[13]. ISO/IEC. (2013). *ISO/IEC 27001:2013S Information security management systems — Requirements*. International Organization for Standardization.

[14]. ISO/IEC. (2018). *ISO/IEC 14443-1/2/3/4: Identification cards — Contactless integrated circuit cards — Proximity cards*. International Organization for Standardization.

[15]. Jain, A. K., Ross, A., & Nandakumar, K. (2016). *Introduction to biometrics*. Springer.

[16]. Jalloh, M. S., & Bamigwojo, O. V. (2023). Data-driven decision support systems for enhancing manufacturing productivity. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *10*(2), 440-449.

[17]. Juels, A. (2006). RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications, 24*(2), 381–394.

[18]. Khan, M. A., Alvi, A. N., & Malik, M. I. (2020). Design and implementation of automated attendance management systems. *International Journal of Advanced Computer Science and Applications, 11*(4), 112–119.

[19]. Kuhn, D. R., Coyne, E. J., & Weil, T. R. (2010). Adding attributes to role-based access control. *Computer, 43*(6), 79–81.

[20]. Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal, 40*(3), 614–634.

[21]. Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *IEEE Computer, 29*(2), 38–47.

[22]. Sanmori, M. T. (2024). AI-Driven Functional Independence Prediction and Assistive Technology Optimization to Reduce Medicare Expenditures Among Older Adults in the United States. International Journal of Scientific Research and Modern Technology, 3(11), 186–205. https://doi.org/10.38124/ijsrmt.v3i11.1295

[23]. Schneier, B., & Kelsey, J. (1999). Secure audit logs to support computer forensics. *ACM Transactions on Information and System Security, 2*(2), 159–176.

[24]. Stallings, W. (2018). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.

[25]. Usoro, S. O. & Amunigun, A.A. (2024). Public–Private Partnerships in Strengthening Rural Food Supply Chains: A Financial and Operational Model for Federal Collaboration, *Int J Sci Res Sci Eng Technol*, vol. 11, no. 2, pp. 645–659, Mar. 2024, doi: 10.32628/IJSRSET2512186.

[26]. Usoro, S. O., Galadima, E. R., & Adogwa, O. H. (2025). Cold Chain Logistics Optimization: Integrating IoT and Data Analytics to Reduce Post-Harvest Loss in the United States Perishable Food Supply Chain: A Case Study of Dole Food Company *International Journal of Scientific Research in Science & Technology*, vol. 12, no. 2, pp. 1452–1468, https://doi.org/10.32628/IJSRST251263207