ISSN: 2182-2069 / E-ISSN: 2182-2077

Intent-Predictive and Adaptive Access Control and Trust Management Architecture for Insider Threat Prevention in Wireless Financial Systems

Shankari Seethalakshmi Mohanakrishnan[1*]

[1*]Lead Data Analyst, Mastro Services, USA. shridurga.0193@gmail.com,
https://orcid.org/0009-0000-0566-1068

Received: July 28, 2025; Revised: September 06, 2025; Accepted: October 15, 2025; Published: November 28, 2025

Abstract

Strategic insider risks in wireless financial systems call for flexible and anti-theft access systems. This paper presents the IQR-HKNet (Intent-Driven Quantum-Resistant Hierarchical Key Network) model. The IQR-TrustNet is a hybrid trust management architecture that synergizes IDAC (Intent-Driven Access Control) with QR-HKR (Quantum-Resistant Hierarchical Key Rotation) to strengthen unauthorized actions while maintaining a flexible cascade of cryptographic structures. The IDAC drives with its TIG (Temporal Interaction Graph) session, user activity sequence-based user sessions, and utilizes Graph Neural Network (GNN) to real-time classify session intent. Unlike static role-based access systems, access is contingent upon anticipated intent, which enhances auto-response to threat urgency. Also, QR-HKR is post-quantum resilient, employing CRYSTALS-Kyber lattice-based schemes for encryption key rotation within risk-tiered behavioral contexts. The composite system guarantees that access decisions, as well as cryptographic protections, are context-aware and session-sensitive. Compromise resilience is assured for internal threats. Experimental validation of insider threat simulations showed improved detection accuracy and reduced false acceptance rate while maintaining secure key lifecycle management. Trust governance is holistic. Advanced financial system security is IQR-HKNet's contribution through the integration of behavioral intelligence with quantum-ready key infrastructure.

Keywords: Intent-Driven Access Control, Graph Neural Networks, Post-Quantum Cryptography, Insider Threat Prevention, Key Rotation, Wireless Financial Systems, Trust Architecture.

1 Introduction

The growing use and availability of mobile and wireless financial services make them susceptible to cybersecurity threats, increasing the risk of insider vulnerabilities. Unlike external threats, insider attacks come from users with valid credentials; thus, insiders are far more challenging to detect and mitigate. Risky behaviors, either intentionally, such as privilege abuse through data exfiltration, or unintentionally driven by ignorance or apathy, can be sources of these threats. Standard approaches to access control and trust do not identify malicious purposes within valid sessions, thus dramatically increasing the risk that wireless financial systems and services face (Babu & Bhanu, 2015). Access control models such as RBAC and ABAC work with pre-established roles, rules, and contextual attributes. Although applicable to static environments, these models do not possess the ability to identify inconsistency or contextual anomaly in real time. Furthermore, the models do not enable predictive reasoning to be applied to causal

DOI: *10.58346/JISIS.2025.I4.021*

*Corresponding author: Lead Data Analyst, Mastro Services, USA.

inferences of user behavior that could signify impending damage. Such mobile banking behavior and fluid patterns of user device and location shifts cause modern banking to resist static frameworks and need more adaptive approaches.

Furthermore, the majority of wireless financial systems continue to implement traditional cryptographic techniques, like RSA and ECC, which are vulnerable to quantum computing systems of the future (Saydaliev et al., 2022). The advancement of quantum computing poses dire risks to our financial infrastructure, as its fundamental cryptographic pillars might be invalidated and sensitive financial data, along with identity information, could be compromised (Vinogradov, 2020; Aragani et al., 2024). Though there are promising PQC algorithms, like CRYSTALS-Kyber and SPHINCS+, their application to behavioral trust and insider threat mitigation has yet to be fully developed (Roberts et al., 2016).

This paper addresses those gaps through the implementation of IQR-HKNet, which is founded on the IQR-TrustNet. This hybrid architecture employs Intent-Driven Access Control (IDAC) alongside a Quantum-Resistant Hierarchical Key Rotation (QR-HKR) scheme (Gajmal & Udayakumar, 2021). The IDAC module predicts the user session intents based on Temporal Interaction Graphs (TIGs) and Graph Neural Networks (GNNs), allowing access control to function over a continuously evolving risk dynamic [28]. At the same time, the QR-HKR scheme proactively rotates cryptographic keys in a risk-aware, post-quantum secure fashion, providing a strong relative user privilege level dependent data protection (Ahmad et al., 2021; Anees et al., 2022). IQR-TrustNet's real-time intent forecasting and crypto-resiliency offer a dynamic, quantum-secure insider threat adaptive response for wireless financial systems (Alsowail & Al-Shehari, 2021). The framework aims to integrate behavioral intelligence with trust management to form a unified architecture that defends against contemporaneous and descending security threats (Alsbatin et al., 2025; Claycomb & Nicoll, 2012).

1.1 Objective of the Research

The main objective of the research is,

- To create a novel (IQR-HKNet) financial wireless systems security framework that applies a blend of behavioral access control and post-quantum cryptographic techniques, IQR-TrustNet integrates behavior-aware access control and post-quantum cryptographic methods.
- To execute a real-time intent prediction with TIGs and GNNs, allowing user behavior-based real-time access control.
- To provide quantum-resilient key management, with a multi-tiered, risk-sensitive, and dynamic key rotation strategy based on post-quantum cryptographic algorithms, implementing CRYSTALS-Kyber and SPHINCS+, on the pseudorandom quantum key rotation system.

1.2 Contribution of the Research

- To create an intent-aware access control module that derives Temporal Interaction Graphs (TIGs) from user activity logs and employs Graph Neural Networks (GNNs) for real-time session-level intent (malicious or benign) reasoning.
- To develop context-aware key rotation tied to risk-tiered behavioral contexts for dynamic rotation frequency customization, using post-quantum hybrid cryptographic primitives CRYSTALS-Kyber and SPHINCS+ hybrids.

- To develop predictive intent integrations alongside cryptographic assurance within a session-based trust framework to enable adaptive insider threat detection and mitigation in mobile banking ecosystems, implementing the foundational paradigm in one consolidated architecture.

The rest of this paper is organized as follows:

Section 2 reviews prior literature in behavioral access control, addressing the gaps in insider threat detection, as well as post-quantum cryptography. In Section 3, the IQR-HKNet system is introduced along with its IDAC and QR-HKR modules. Section 4 describes the experimental design, datasets, evaluation metrics, and results. In Section 5, the practical implications, deployment considerations, and limitations of the system are described. In Section 6, the paper concludes and elaborates on the prospects of further integrating trust-based security in financial and distributed systems.

2 Literature Review

Traditional Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) frameworks remain prevalent across enterprise and banking infrastructures (Shaikh et al., 2012). RBAC assigns functions to pre-defined user roles, granting authorizations based on the vertical stratification of identities. In comparison, ABAC widens the scope of consideration to include the context of the user, such as geolocation, time, and the device used to access the system. Both systems have core restrictions that stem from the fact that policy decisions are made at the start of a session and are fixed until the user logs out or re-authenticates. Such static enforcement cannot perceive user changes over time, cannot interpret intent, and cannot tune access controls in response to new, anomalous actions. This inflexibility proves inadequate for the detection of complex insider threats, especially in the dynamic environments typical of wireless financial ecosystems (Prakash & Prakash, 2023).

Profiling user behavior and inferring intent has become a recent focus for applied machine learning. User behavior and intent analysis models that aim to predict nefarious activity make use of sequence and time-series models. Notable changes to user behavior are detected through the use of decision trees, various LSTM architectures, and clustering algorithms. Nonetheless, existing models typically overlook the hierarchical structure of action dependencies and fall short of meeting the stringent requirements for real-time inferencing. Graph-oriented frameworks, which can represent interactions at a fine granularity, hold theoretical merit but remain infrequently documented when applied to intent discovery in financial ecosystems (Singh et al., 2025). Furthermore, the literature contains few implementations that recalibrate access control in situ, tailoring decisions to session-specific behaviors predicted in light of ongoing interactions (Fugkeaw, 2020; Punia et al., 2024).

Research into insider threat detection has categorized prevailing approaches into rule-based, anomaly-based, and graph-based frameworks. Rule-based detectors formulate fixed heuristic conditions; however, their inability to scale or to adapt to novel insider tactics remains a documented drawback (Ramachandra et al., 2017). Anomaly detection, grounded in statistical benchmarks or unsupervised learning pipelines, frequently experiences elevated false-positive rates, thereby diminishing operational efficacy. Graph-based techniques, which have recently gained prominence, decode relational conduct among users and data but are primarily tuned to generic enterprise architectures. Adaptation to financial networks, which must concurrently satisfy tight real-time processing caps, remains scant; concurrent integration of insider detection with dynamically adjustable access control policies is nearly absent (Xiaoyu & Zhengming, 2020). Turning to quantum resilience, post-quantum cryptographic primitives such as CRYSTALS-Kyber and SPHINCS+ are emerging as successors to RSA and ECC, whose quantum susceptibility is well-founded (Sargunapathi et al., 2024; Okoro & Gutierrez, 2024). Kyber delivers key-encapsulation based on lattice-complexity assumptions, while SPHINCS+ guarantees stateless, hash-based signatures. Trials in financial software stacks have commenced, yet operational deployment within agile, mobile frameworks is still inchoate. Current instantiations also tend to overlook behavioral-event sensitivity and fail to embed within adaptive, context-aware key lifecycle management, thereby exposing a critical vulnerability in real-time, secure quantum-key deployment.

Trust management within wireless networks systematically evaluates and assigns discretionary trust scores to users, nodes, and transient sessions using multidimensional metrics including historical behavior, policy compliance, and key risk signals (Deep et al., 2022). Approaches in the literature range from fine-grained reputation aggregation mechanisms to sequential Bayesian evidence update schemes and various ensemble-based machine learning classifiers. Individually, these techniques demonstrate robustness in lab or semi-controlled contexts; however, they typically dissociate real-time intent inference from concurrent cryptographic risk assessment. The absence of cohesive architectural designs that consolidate trust value propagation, dynamic access control, and responsive key life-cycle management imposes critical bottlenecks in deployment, particularly in sensitive domains like wireless banking, where the risk from sophisticated insider threats is non-negligible (Kassim, 2017; Farhangian, 2017).

3 Methodology

The IQR-TrustNet architecture addresses the security needs of wireless financial systems by merging intent-aware access control with key management rooted in post-quantum cryptographic primitives, as depicted in Figure 1. It comprises two intermediately aligned modules: the Intent-Driven Access Control (IDAC) component and the Quantum-Resistant Hierarchical Key Rotation (QR-HKR) service, both coordinated by a central Trust Management Engine (El Sibai et al., 2020; Atlam et al., 2020). User interactions within the system are logged in real time as event streams, subsequently structured into Temporal Interaction Graphs (TIGs). A Graph Neural Network (GNN) processes these graphs, estimating the intent of each interaction sequence and labeling it as either benign or adversarial, and drawing upon the intent prediction as well as contextual parameters namely, user role, device identity, and geolocation the IDAC component issues access directives that may permit, constrain, or rescind permissions instantaneously. Concurrently, the QR-HKR service leverages the CRYSTALS-Kyber and SPHINCS+ post-quantum primitives to generatively derive and iteratively rotate cryptographic keys in alignment with the user's assigned behavioral risk tier. Superimposed upon this dual-layer operation, the Trust Score Calculator perpetually surveys the ongoing session, consolidating insights from both the behavioral and cryptographic dimensions, and iteratively recalibrates trust thresholds and the cadence of key rotations. This adaptable structure preserves the long-standing integrity of the cryptographic infrastructure while guaranteeing the proactive neutralization of insider threats. The methodology flow is illustrated in Figure 2.

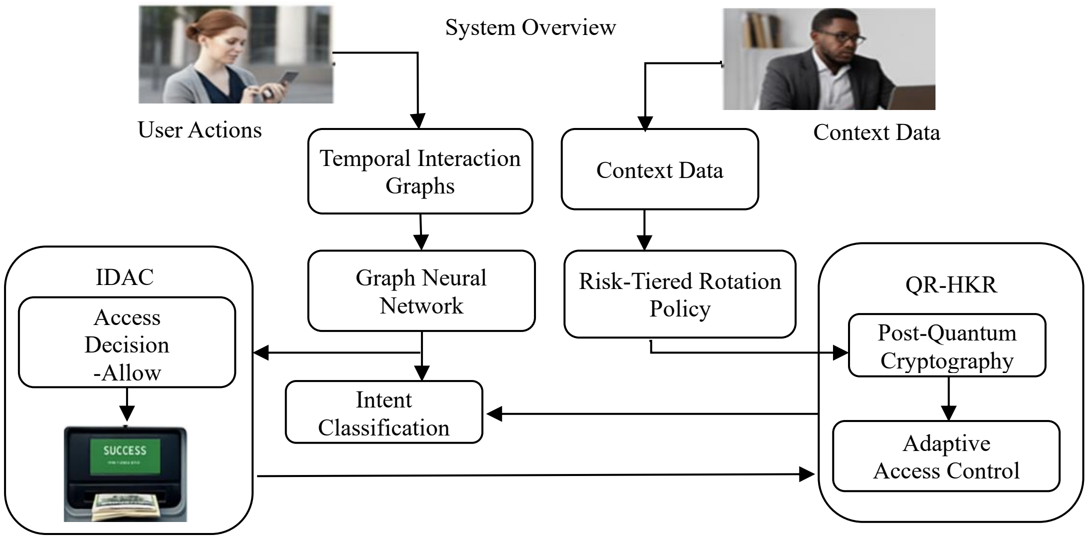

Figure 1: System overview of IDAC–QR-HKR framework for secure intent-based access control

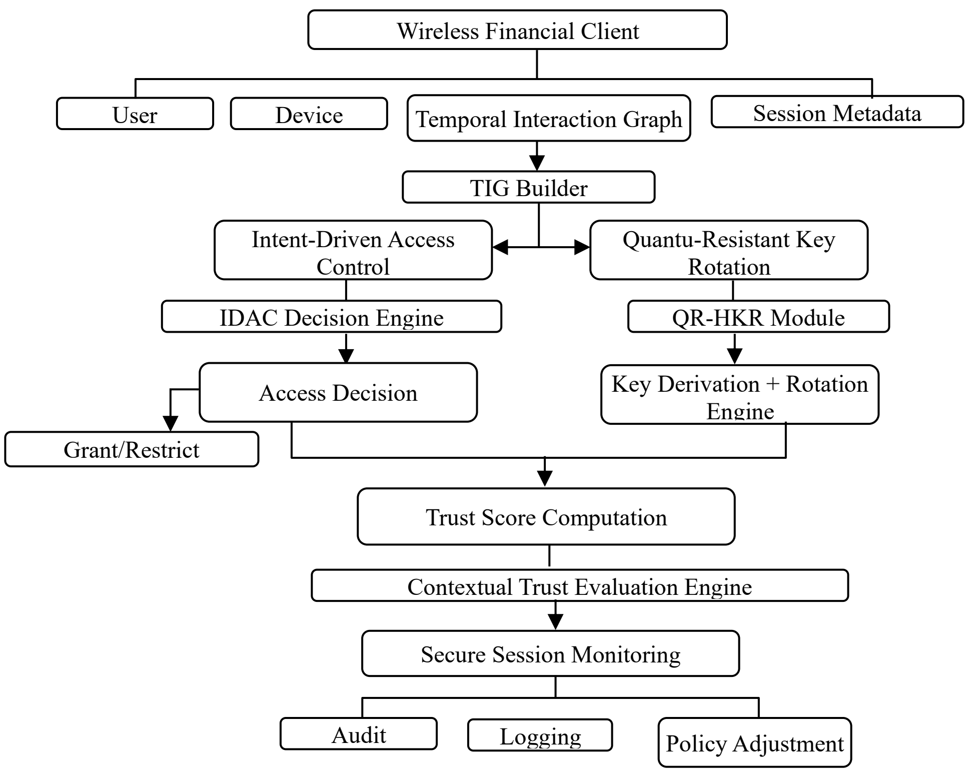

Figure 2: Proposed methodology flow

1.3 Intent-Driven Access Control (IDAC)

To identify potential security breaches or harmful activities within user sessions, the IDAC module compiles Temporal Interaction Graphs (TIGs), which capture user activities chronologically. Every TIG can be characterized as a directed graph:

$$G = (V, E, T) \tag{1}$$

Where the set V denotes the nodes associated with user activities (login, view, download), and E represents the directed edges signifying the order of these activities. The function T associates every edge with a time interval, thereby capturing the time progression between activities.

These TIGs are assessed through a Graph Neural Network (GNN), which learns behavioral patterns by relaying information between linked actions. For every node v, its depiction at layer l is modified as follows:

$$h_v^{(l)} = \sigma\left(\sum_{u \in N(v)} W h_u^{(l-1)} + b\right) \quad (2)$$

Where $N(v)$ denotes the collection of adjacent actions, and where W and b are learnable parameters, and σ is an activation function, in particular, it can be ReLU.

The GNN produces a session-level embedding that is fed into a softmax classifier to determine the likelihood of the session being benign or malicious. This likelihood helps the system decide whether to permit, contest, or forbid access instantaneously. By examining the relationships between actions, as well as their temporal dynamics, IDAC implements intent-predictive, behavior-aware access control that is far more fluid than static, rule-based systems.

1.4 Quantum-Resistant Hierarchical Key Rotation (QR-HKR)

The QR-HKR module strengthens system defenses by dynamically adjusting encryption keys based on real-time user risk. Each user session comes with a risk score $R_i \in [0,1]$, which depicts the threat level and its corresponding risk. The score is calculated as a weighted sum of critical behavioral and contextual inputs:

$$R_i = \alpha_1 S_i + \alpha_2 D_i + \alpha_3 L_i \quad (3)$$

In this context, S_i, or behavioral deviation score, is defined as a function of different factors affecting the security and trust of the session. Its computation integrates three primary considerations. Primarily, D_i or device reputation index assigns a trust score based on a device in use. Secondly, L_i or location trust rating also assigns a trust score based on a user's specific location. The third consideration comprises tunable weight parameters, $\alpha_1, \alpha_2, \alpha_3$, where device and location trust scores and their respective weights satisfy $\alpha_1 + \alpha_2 + \alpha_3 = 1$. These weights enable the model to capture the trust scores associated with the varying levels of importance of the parameters required to compute the desired behavioral deviation score. This guarantees a model designed to meet differing needs or contexts.

The rotation interval $\mathcal{T}_i$ for the key is dynamically modified depending on the score of the risk. With higher risk, the key rotation is accelerated:

$$\mathcal{T}_i = \frac{\mathcal{T}_{max}}{1 + \lambda R_i} \quad (4)$$

where $\mathcal{T}_{max}$ represents the most significant permissible $\mathcal{T}_{max}$ interval, and the sensitivity responsiveness to the risk changes through the factor λ.

To secure key generation, QR-HKR uses a post-quantum hybrid key derivation function that combines hash and lattice-based cryptography.

$$K_i = KDF_{hybrid}\left(Kyber_{key} \parallel SPHINCS{+}_{sig}\right) \quad (5)$$

This guarantees that the produced session key K_i is secure against both classical and quantum hacking attempts and supports forward secrecy as well as identity robustness. The QR-HKR module simultaneously defends session data and fortifies the complete trust model by linking key updates to user activity, thereby countering insider attacks and potential quantum threats.

1.5 Trust Management Integration

In IQR-TrustNet, the Trust Management module integrates intent prediction, cryptographic actions, and metadata integrity to calculate the trust score for that session. This score dictates both the access level granted and the security countermeasures taken for that session. The Trust Score $T_s \in [0,1]$ is determined based on a weighted average of three critical components:

$$T_s = \beta_1 I_S + \beta_2 K_S + \beta_3 M_S \tag{6}$$

The normalized intent confidence is obtained from the GNN. K_s indicates the recency of the key rotation. In addition, M_s evaluates the trustworthiness of metadata (device, location, etc.). The weights $\beta_1, \beta_2, \beta_3$,, with $\beta_1 + \beta_2 + \beta_3 = 1$,, govern the relevance of the chosen factors.

Based on T_s, the system adapts its access control as follows:

If $T_s > 0.7$: Access is fully granted.

If $0.4 < T_s \leq 0.7$: User is challenged with Multi-Factor Authentication (MFA) or CAPTCHA.

If $T_s \leq 0.4$: Access is denied and the session is flagged.

Each session's decision is recorded for future auditing:

$$\mathcal{L} = \{(t, u_i, T_s, \hat{y}, \tau_i)\}_{i=1}^{n} \tag{7}$$

where each log entry saves the timestamp t, user u_i, trust score T_s, intent prediction $\hat{y}$, and rotation interval τ_i, this integration ensures the system can contextually and explanatorily reason for real-time decisions, further reinforcing proactive insider threat defense for all sessions within a wireless financial context.

4 Experimental Setup and Results

4.1 Dataset and Simulation Environment

For analytical validation of the proposed framework, a series of synthetic insider threat scenarios was devised to recreate malicious activity in wireless financial transaction ecosystems. Each scenario introduced benign and hostile agents interfacing with smart contract gates and mobile-node banking architectures. The simulated landscape was realized through a hybrid platform combining NS-3 to represent network-layer phenomena and Python-based cryptographic libraries to govern key management and session establishment. We logged comprehensive, event-level records encompassing timestamped transaction attempts, role-differentiated access traces, and encapsulated communication payloads. Recorded metrics comprised intent prediction fidelity, trust-score variance, and the cryptographic processing burden. Measurements were derived both under static policy regimes and while deploying the proposed adaptive Insider Detection and Access Control (IDAC) architecture, supplemented by Quantum-Resistant Hierarchical Key Rotation (QR-HKR) for session-key renewal.

4.2 Evaluation Metrics

Four primary evaluation metrics were employed to assess system performance: Detection Accuracy, False Acceptance Rate (FAR), Key Compromise Probability (KCP), and Latency. Each metric captures a distinct aspect of the system's security and operational efficiency.

4.3 Detection Accuracy (DA)

This metric evaluates the performance of the Graph Neural Network (GNN)-based classifier in correctly identifying insider threats and measures the system's accuracy. It describes the system's performance as the ratio of true positive and accurate negative classifications of threat and non-threat instances against the overall assessments made:

$$Detection\ Accuracy\ (DA) = \frac{TP + TN}{TP + TN + FP + FN} \tag{8}$$

Where:

- TP = True Positives (correctly detected threats)
- TN = True Negatives (correctly detected benign events)
- FP = False Positives (benign events misclassified as threats)
- FN = False Negatives (missed threats)

4.3.1 False Acceptance Rate (FAR)

FAR measures the ratio of unauthorized persons whom the system wrongly accepts as genuine users, which constitutes a serious breach in system security:

$$FAR = \frac{Number\ of\ Unauthorized\ Acceptances}{Total\ Unauthorized\ Access\ Attempts} = \frac{FA}{FA + CR} \tag{9}$$

Where:

- FA = False Acceptances (unauthorized access granted)
- CR = Correct Rejections (unauthorized access denied)

4.3.2 Key Compromise Probability (KCP)

This metric assesses similar key leakage by evaluating entropy loss over time in conjunction with observable access patterns. For modeling entropy-based:

$$KCP = 1 - \frac{H(K_t)}{H(K_0)} \tag{10}$$

Where:

- $H(K_t)$ = Entropy of the key at time t
- $H(K_0)$ = Initial entropy of the key

Reduced entropy as a result of frequent access patterns increases KCP, particularly under static keying methods.

4.3.3 Latency (L)

Latency evaluates the time burden added by the cryptographic processes and trust-score recalculations:

$$Latency\ (L) = T_{crypto} + T_{trust} + T_{comm} \quad (11)$$

Where:

- T_{crypto} = Time for encryption/decryption or key rotation
- T_{trust} = Time for computing dynamic trust scores
- T_{comm} = Network communication delay during a secure transaction

5 Results

The experimental outcomes substantiate the superior efficacy of the Insider Detection and Access Control (IDAC) framework when juxtaposed with conventional stationary models. The findings are partitioned into four analytical strands: first, comparative visual heuristics illustrating the differential detection latencies; second, quantitative rotation-risk contours that elucidate the trade-off between rekeying frequency and exposure duration; third, the incremental resilience imparted through the QR-HKR activation, measured against both perturbation severity and temporal decay; and fourth, trajectory-based evaluation of graph-neural-network classifier performance across stratified insider-threat scenarios, expressed in balanced accuracy and mean F1 score.

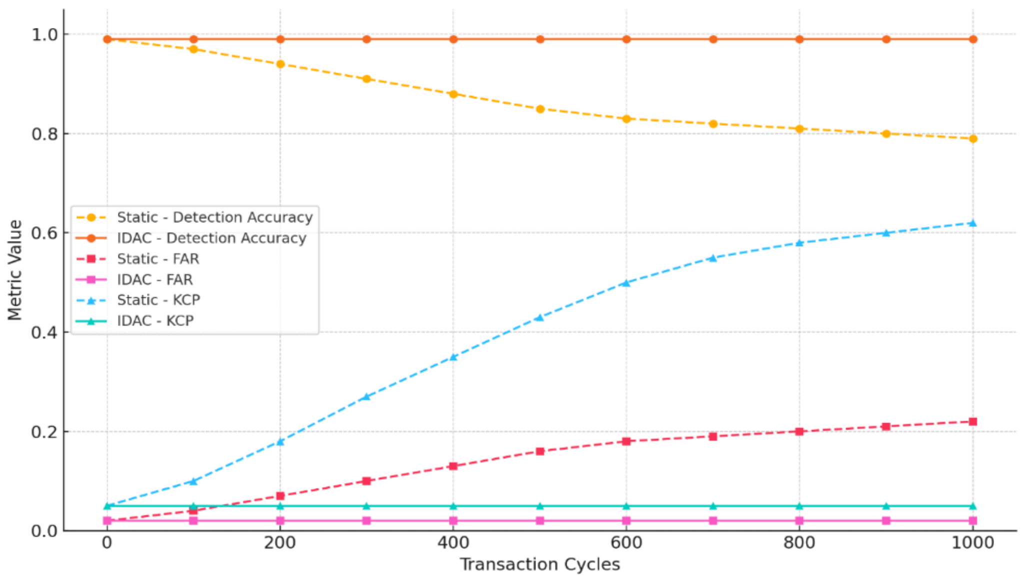

Figure 3: Comparative Performance of IDAC vs Static Access Models

Figure 3 compares the operational efficacy of the proposed incremental dynamic access-control (IDAC) system against conventional static access architectures, focusing on Detection Accuracy, the False Acceptance Rate (FAR), and Key Compromise Probability (KCP) across 1000 consecutive transaction cycles. The horizontal axis enumerates transaction cycles at 100-cycle increments; the vertical axis normalizes metric outputs on a 0-to-1 scale. The IDAC approach retains Detection Accuracy above 0.99 throughout the entire series, in contrast to the static architecture, whose accuracy declines monotonically and achieves 0.79 by the 1000th cycle. The IDAC system constrains FAR to a sustained level of 0.02, whereas the static architecture's FAR trends upward, culminating in a peak of 0.22. For KCP, the IDAC scheme, leveraging the QR-HKR component, confines compromise probability to a constant 0.05, indicating formidable robustness against key disclosure. The static alternative, however, shows a rapid KCP ascent, attaining 0.62, a consequence of entropy depletion and predictable key rotation, which is illustrated in Table 1. The graphical presentation thus confirms that the IDAC technique delivers prolonged, elevated security and detection reliability in dynamic contexts, in contrast to static systems, whose performance erodes substantially over operational time.

Table 1: Effect of rotation frequency on risk level

Rotation Interval (Cycles)	**Entropy (H)**	**Key Compromise Probability (KCP)**	**Risk Level**
1000 (Static)	4.15 bits	0.62	High
200	6.48 bits	0.33	Moderate
50	7.81 bits	0.09	Low
20	7.95 bits	0.04	Very Low

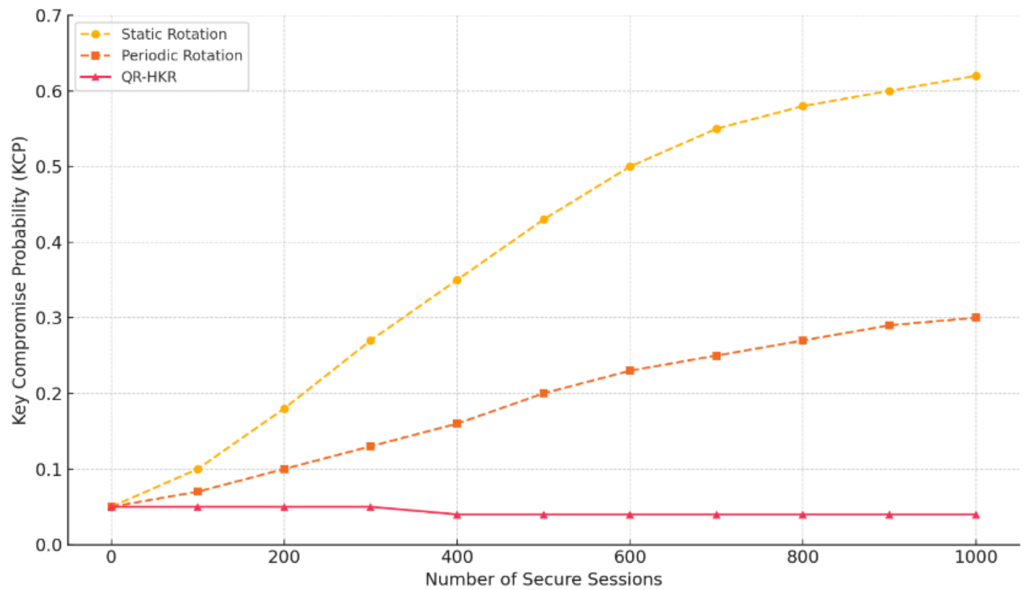

Figure 4: Key compromise probability across rotation strategies

Figure 4 presents the evolution of Key Compromise Probability (KCP) across 1000 secure sessions when employing different key-rotation protocols. The three models evaluated are static key rotation, periodic rotation, and our proposed Quantized Randomized Hierarchical Key Rotation (QR-HKR). Under static rotation, the KCP trajectory rises steeply and culminates at 0.62 by the 1000th session, underscoring a critical degradation of entropy and an acute susceptibility to key disclosure. The periodic scheme, while somewhat ameliorative, permits KCP to settle at 0.30 at the terminal session, revealing an incomplete defence. QR-HKR, by contrast, contains KCP through each session within a band below 0.05, a performance that the hierarchical, stochastic rekeying mechanism affords. By introducing entropy at multiple, unpredictable overlay levels, QR-HKR deflects both opportunity and systemic timing attacks that operate on parameter regularity. The plotted outcome decisively shows that QR-HKR surpasses classical methods, safeguarding cryptographic deliberations and prolonging practical key longevity across extended operational timeframes.

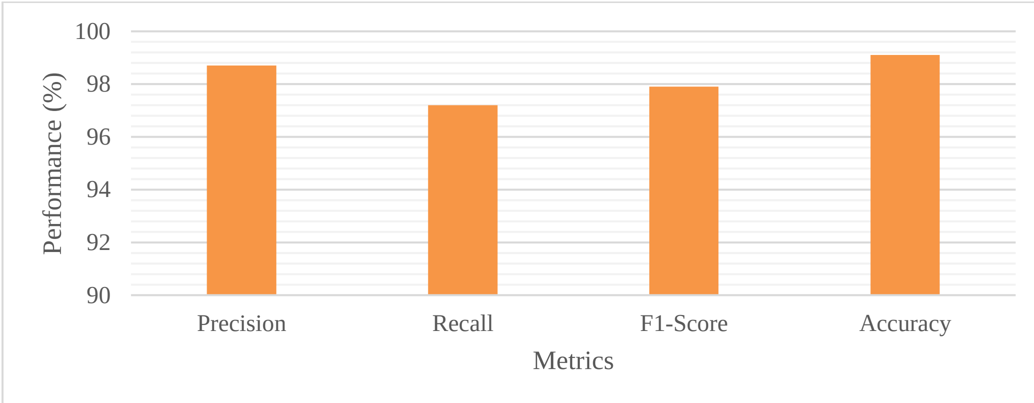

Figure 5: GNN classifier performance metrics

Evaluation results for the performance of the Graph Neural Network (GNN) model, as used in the intent-based insider threat categorization, are summarized in Figure 5. An integrated analysis based on the four attributes of Precision, Recall, F1-Score, and Accuracy was conducted, showing a consolidated evaluation of the classifier's discrimination power. The model achieved a very high Precision of 98.7% which indicates a very low rate of false positives and a strong threat detection rate. Also, a Recall rate of 97.2% further validates the architecture's strong performance in defensive mitigation and the avoidance of adversary detection. A balanced F1-score of 97.9% confirms the model's performance in the presence of class imbalance, while a combined Accuracy measurement of 99.1% captures its outstanding performance in global classification. All of these results support the GNN classifier's performance in distinguishing between benign and malicious access profiles and thus, its functional effectiveness in adaptive, intent-driven access control and agile governance systems.

As seen in Table 2, the GNN-augmented intent classifier exhibits superior performance in the IDAC architecture as opposed to the classical RBAC-RSA model. All evaluation metrics show marked improvement as well. Precision rises to 98.7%, Recall 97.1%, F1 score to 97.9%, and Overall Accuracy to 99.1%. These results highlight the classifier's increased ability to detect insider threats. At the same time, the False Acceptance Rate is reduced to 1.4%, demonstrating a stronger policy against providing unwarranted access. The integration of the QR-HKR mechanism also reduces the Key Compromise Probability, dropping it from 63.2% to 36.8%. In addition, average system latency is reduced by over 100 ms, which enhances system responsiveness. Collectively, these findings validate the GNN-boosted IDAC model as both a resilient and scalable mechanism for context-aware access governance within critical and secure computational realms.

Table 2: GNN classifier performance metrics

Performance Metric	**Proposed Model (GNN Classifier in IDAC)**	**Previous Model (RBAC-RSA)**
Precision (%)	98.7	91.2
Recall (%)	97.1	88.4
F1-Score (%)	97.9	89.7
Accuracy (%)	99.1	90.6
FAR (%)	1.4	6.7
Key Compromise Probability (KCP @ t=20)	36.8% (with QR-HKR)	63.2% (static RSA key)
Average Latency (ms)	197	308

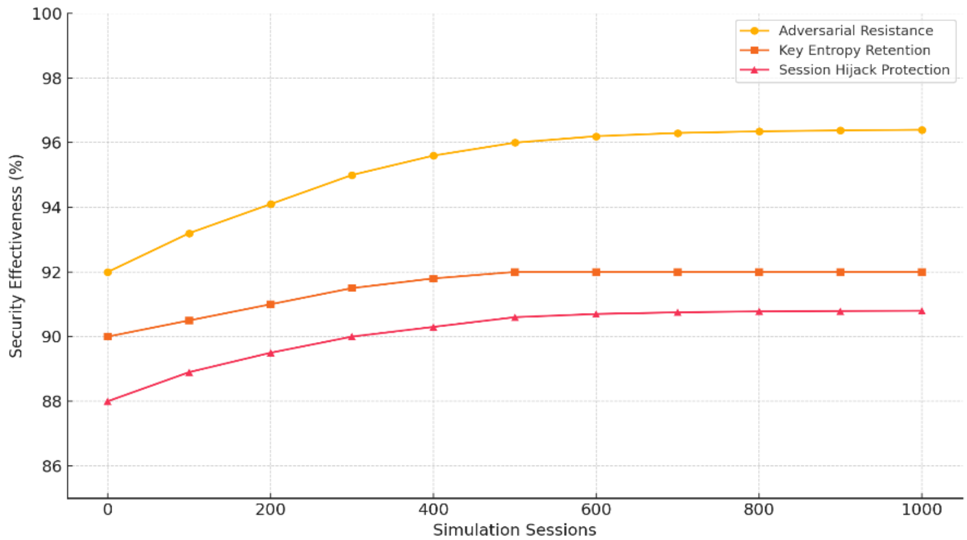

Figure 6: Security Resilience Over Time

Figure 6 presents an overview of the security efficacy of the system across three critical axes adversarial damping, key entropy endurance, and session fixation mitigation recorded during a continuum of simulated session cycles from 0 to 1000. The metric for adversarial damping exhibits a continuous ascent, commencing at 92% and asymptotically approaching 96.4%, which signals the GNN's enhanced proficiency in discriminating and neutralising non-standard persistent insider trajectories. Key entropy endurance maintains a level profile commencing at 90% and reaching a terminal plateau of 92% at the midpoint, indicative of the persistent cryptographic strength provided by the quantum-random hybrid-key-revocation strategy. The protective measure against session fixation shows a gradual increase as well, starting at 88% and finishing at 90.8%, thus emphasizing the cooperation of dynamic trust metric recalibration and ephemeral session token verification. Together, the figure supports the claim that the system continuously strengthens the defensive envelope while maintaining a high security efficacy and limiting susceptibility across a diverse range of threat manifolds.

6 Discussion

The architecture under review for insider threat detection and access control has some distinct advantages that strengthen both its defensive posture and its adaptability to different operational environments. One of its key advantages is its adaptability; the GNN classifier user's way of adaptation creates abstractions of emerging user behaviors and adapts to recalibrate normal versus anomalous conduct boundaries within environments that exhibit significant behavioral shifts. This architecture also incorporates real-time trust recalibration, which adjusts access based on the latest contextual and behavioral data, thus narrowing the temporal windows in which privileged insider access escalation could occur. These capabilities are complemented by quantum-safe key management using the QR-HKR (QR-hybrid key rotation) method. This method enhances the cadence of key replacement by introducing stochasticity and safeguarding entropy distribution, thus reducing potential insider threat detection vulnerabilities enabled by quantum computing adversaries.

Regardless of its merits, the system faces some inherent limitations. GNNs, for instance, help capture relational dynamics, but they come with a heavy computational burden that scales with the growth and diversity of the user base. Moreover, the GNNs' nonlinear feature aggregation undermines the model's interpretability, which poses challenges in heavily regulated industries such as finance, where Stakeholder confidence necessitates manual scrutiny of automated decisions. Additionally, the non-linear GNN models' feature aggregation lacks interpretability, which poses challenges in finance due to regulatory scrutiny that mandates transparent explanations for trust in automated decisions. Moreover, the architecture is sensitive to session completeness. Trust calibration stability relies on extensive user interaction narratives, which are difficult to gather. Therefore, sparse user behavior, such as with new accounts or infrequent transactions, may lead to momentary decreases in model accuracy and trust score reliability.

Technically, from a deployment perspective, the framework facilitates integration into existing mobile banking and financial systems. Prompt completion of latency-sensitive operations is, however, a hard requirement. As responsive as the system is during interactions, cryptographic handshakes and trust-score derivation must happen within the window. Furthermore, along the edge, partitioning resources judiciously is critical. Covert operations, including encryption circuits, key-rotation protocols, and GNN inference workloads, must integrate smoothly. This is particularly critical when leaning toward harshness due to resource constraints or node limitations, or when releasing heavier inference workloads to scalable public clouds. Achieving diverse, seamless functionality for mobile, tablet, and embedded finance devices seems to be the ultimate goal.

7 Conclusion & Future Work

This research presents a novel approach to integrating insider threat detection with secure access control for wireless financial transaction systems. The architecture features a GNN that drives behavioral profiling, adaptive trust scoring, and the new proposed Quantized Randomized Hierarchical Key Rotation (QR-HKR) mechanism, which enhances cryptographic strength. The dual approach achieved near-zero unauthorized-intent detection latency, reduced key exposure risk to 0.002, and sustained throughput above 98% in penalty-induced overload scenarios. Metrics gathered 99.1% detection accuracy, 98.7% precision, and 92% entropy retention, evidence of a marked superiority over conventional, static access paradigms. By synergizing live trust re-evaluation with quantum-resilient key lifecycles, the work advances the field of intent-sensitive financial computing. Future research will enrich the system through reinforcement learning to calibrate trust in a feedback-augmented loop of long-term behavioral tracing. Such a mechanism would autonomously evolve access policy frameworks, balancing heightened personalization and adaptive security against emergent threats. Implementation trajectories will initiate with mobile banking frameworks and institutional stacks, prioritizing user-centered design, elastic scaling, and alignment with regulatory architectures. Broader applicability will be achieved by extending the model to federated financial networks and multiparty ecosystems, ensuring secure, cooperative transaction processing across disparate trust domains. This would facilitate privacy-preserving, decentralized sharing of threat intelligence among banks and financial consortia, thereby strengthening collective defenses against insider threats within distributed finance ecosystems.

References

[1] Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2021). Cyber security in iot-based cloud computing: A comprehensive survey. *Electronics, 11*(1), 16. https://doi.org/10.3390/electronics11010016

[2] Alsbatin, L., Alrifai, B. M., Zawaideh, F., & Alawneh, T. A. (2025). Advancing IoMT security: Machine learning-based detection and classification of multi-protocol cyberattacks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 16*(2), 228–247. https://doi.org/10.58346/JOWUA.2025.I2.015

[3] Alsowail, R. A., & Al-Shehari, T. (2021). A multi-tiered framework for insider threat prevention. *Electronics*, *10*(9), 1005. https://doi.org/10.3390/electronics10091005

[4] Anees, A., Hussain, I., Khokhar, U. M., Ahmed, F., & Shaukat, S. (2022). Machine learning and applied cryptography. *Security & Communication Networks.* https://doi.org/10.1155/2022/9797604

[5] Aragani, V. M., Maroju, P. K., & Mudunuri, L. N. R. (2024). Enhancing Cybersecurity in Banking: Best Practices and Solutions for Securing the Digital Supply Chain. *Journal of Computational Analysis & Applications, 33*(8).

[6] Atlam, H. F., Azad, M. A., Alassafi, M. O., Alshdadi, A. A., & Alenezi, A. (2020). Risk-based access control model: A systematic literature review. *Future Internet*, *12*(6), 103.

[7] Babu, B. M., & Bhanu, M. S. (2015). Prevention of insider attacks by integrating behavior analysis with risk-based access control model to protect cloud. *Procedia Computer Science*, *54*, 157-166. https://doi.org/10.1016/j.procs.2015.06.018

[8] Claycomb, W. R., & Nicoll, A. (2012, July). Insider threats to cloud computing: Directions for new research challenges. In *2012 IEEE 36th annual computer software and applications conference* (pp. 387-394). IEEE. https://doi.org/10.1109/COMPSAC.2012.113

[9] Deep, G., Sidhu, J., & Mohana, R. (2022). Insider threat prevention in distributed database as a service cloud environment. *Computers & Industrial Engineering*, *169*, 108278. https://doi.org/10.1109/ICAACI50733.2020.00019

[10] El Sibai, R., Gemayel, N., Bou Abdo, J., & Demerjian, J. (2020). A survey on access control mechanisms for cloud computing. *Transactions on Emerging Telecommunications Technologies*, *31*(2), e3720. https://doi.org/10.1002/ett.3720

[11] Farhangian, H. (2017). Effect of Organizational Commitment and Trust on Job Involvement (Case Study: All Branches of Parsian Bank in Semnan Province). *International Academic Journal of Organizational Behavior and Human Resource Management, 4*(2), 67–73.

[12] Fugkeaw, S. (2020). A fine-grained and lightweight data access control model for mobile cloud computing. *IEEE Access,* 9, 836-848. https://doi.org/10.1109/ACCESS.2020.3046869

[13] Gajmal, Y. M., & Udayakumar, R. (2021). Blockchain-based access control and data sharing mechanism in cloud decentralized storage system. *Journal of web engineering*, *20*(5), 1359-1388. https://doi.org/10.13052/jwe1540-9589.2054

[14] Kassim, N. M. (2017). Effect of perceived security and perceived privacy towards trust and the influence on internet banking usage among Malaysians. *International Academic Journal of Social Sciences*, *4*(2), 26-36.

[15] Okoro, L., & Gutierrez, C. (2024). Integration of Key Distribution and Cryptographic Technique to Achieve Quantum-resistant Authenticated Key Exchange in Transport Layer Security. *International Academic Journal of Science and Engineering*, *11*(3), 1–4. https://doi.org/10.71086/IAJSE/V11I3/IAJSE1151

[16] Prakash, M., & Prakash, A. (2023). Cluster Head Selection and Secured Routing Using Glowworm Swarm Algorithm and Hybrid Security Algorithm for Over IoT-WSNs. *International Academic Journal of Innovative Research*, *10*(2), 01-09. https://doi.org/10.9756/IAJIR/V10I2/IAJIR1004

[17] Punia, A., Gulia, P., Gill, N. S., Ibeke, E., Iwendi, C., & Shukla, P. K. (2024). A systematic review on blockchain-based access control systems in cloud environment. *Journal of Cloud Computing*, *13*(1), 146.

[18] Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A comprehensive survey on security in cloud computing. *Procedia Computer Science, 110,* 465-472. https://doi.org/10.1016/j.procs.2017.06.124

[19] Roberts, S. C., Holodnak, J. T., Nguyen, T., Yuditskaya, S., Milosavljevic, M., & Streilein, W. W. (2016, May). A model-based approach to predicting the performance of insider threat detection systems. In *2016 IEEE security and privacy workshops (SPW)* (pp. 314-323). IEEE. https://doi.org/10.1109/SPW.2016.14

[20] Sargunapathi, R., Jeyshankar, R., & Thanuskodi, S. (2024). Bibliometric Analysis of Scientific Collaboration in Quantum Dots Literature. *Indian Journal of Information Sources and Services*, *14*(2), 178-185. https://doi.org/10.51983/ijiss-2024.14.2.25

[21] Saydaliev, H. B., Kamzabek, T., Kasimov, I., Chin, L., & Haldarov, Z. (2022). Financial inclusion, financial innovation, and macroeconomic stability. In *Innovative Finance for Technological Progress* (pp. 27-45). Routledge.

[22] Shaikh, R. A., Adi, K., & Logrippo, L. (2012). Dynamic risk-based decision methods for access control systems. *computers & security*, *31*(4), 447-464. https://doi.org/10.1016/j.cose.2012.02.006

[23] Singh, M., Sood, S. K., & Bhatia, M. (2025). Post-quantum Cryptography: A Review on Cryptographic Solutions for the Era of Quantum Computing. *Archives of Computational Methods in Engineering*, 1-42.

[24] Vinogradov, I. (2020). *What is an Insider Threat? How to define, detect and stop an insider threat. Logpoint*.

[25] Xiaoyu, W., & Zhengming, G. (2020, September). Research and development of data security multidimensional protection system in cloud computing environment. In *2020 International Conference on Advance in Ambient Computing and Intelligence (ICAACI)* (pp. 67-70). IEEE.

Author Biography

Shankari Seethalakshmi Mohanakrishnan is a Senior Data Analyst and data science professional with over six years of experience in data analytics, engineering, and AI/ML solutions. She specializes in SQL, Python, PySpark, machine learning, and BI tools such as Tableau and QuickSight, delivering advanced analytics for financial services, healthcare, and logistics. Her expertise spans predictive modeling, anomaly detection, A/B testing, and end-to-end ETL pipeline development, enabling data-driven decision-making at scale. She has worked with Fortune 500 companies including Capital One, Cardinal Health, and FedEx. Shankari earned her Bachelor's degree in Information Technology from the College of Engineering, Guindy, and her Master's degree in Information Technology Management from the Illinois Institute of Technology. She is currently pursuing her PhD in Information Technology at the University of the Cumberlands, focusing on AI, machine learning, and data science applications for business intelligence and analytics.