Article

Not peer-reviewed version

# A Multi-Layered Security Model: The Human Factor, Identification, and Secure Network Communications

Zhuldyz Tashenova *, Askhatov Alim, Gabdullin Abzal, Abdikhaimov Yelnur, Raiskanov Rassul, Oryntay Al-Tarazi, Zhanat Abdugulova *, Shirin Amanzholova

Posted Date: 5 February 2026

doi: 10.20944/preprints202602.0450.v1

Keywords: multi-layer security; defense-in-depth; IoT; SCADA; Zero Trust; human factors

*Article*

# A Multi-Layered Security Model: The Human Factor, Identification, and Secure Network Communications

**Zhuldyz Tashenova [1], Askhatov Alim [2], Gabdullin Abzal [3], Abdikhaimov Yelnur [3], Raiskanov Rassul [3], Oryntay Al-Tarazi [3], Zhanat Abdugulova [3,*] and Shirin Amanzholova [4]**

[1] PhD, Department of Information Security System, Faculty of Information Technologies L. N. Gumilyov Eurasian National University, 11 Alexander Pushkin Street, Astana, Kazakhstan

[2] Master's student in Information Security Systems (ISS),

[3] Department of Information Technologies, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan;

[4] Department of Information Technologies, Kurmangazy Kazakh National Conservatory, Astana, Kazakhstan

* Correspondence: janat_6767@mail.ru

**Abstract**

Modern cybersecurity challenges span multiple layers, from human behavior and identity management to network communication and device security. This paper proposes a unified multi-layered security framework that integrates human-centric, identity-centric, and communication-centric defenses into a coherent architecture. Drawing on insights from diverse domains (industrial control systems, IoT, healthcare, blockchain, and quantum communications), we identify common defense-in-depth principles and interdependencies across layers. The study highlights the persistent gaps in current research, which often focuses on isolated layers or domain-specific models, and addresses these gaps by synthesizing a cross-domain framework. We develop a mixed-method methodology to compare and integrate multi-layer security mechanisms, and we implement a proof-of-concept risk assessment engine to evaluate the framework's effectiveness. Preliminary results from this implementation demonstrate that combining layers yields significantly improved detection performance and resilience compared to single-layer baselines. The framework's contributions include a comprehensive literature-driven model, an operational validation in a simulated environment, and guidelines for deploying multi-layer defenses in complex, interconnected infrastructures. Empirical findings confirm that an integrated multi-layer approach can adapt to varied threat scenarios and reduce vulnerabilities, underscoring the value of coordinated controls across technical and human factors. The proposed framework lays a foundation for future work on scalable, cross-layer cybersecurity architectures that better protect contemporary cyber-physical systems.

**Keywords:** multi-layer security; defense-in-depth; IoT; SCADA; Zero Trust; human factors

## 1. Introduction

Modern systems increasingly demand a multi-layered security approach that integrates defenses across all levels, from human factors to device hardware. Recent studies confirm this trend: a survey of IoT architectures highlights the need for cross-layer protections in resource-constrained devices [1], and real-world industrial cases show that many SCADA/CPPS components still operate without basic safeguards (encryption, strong authentication) [9]. These findings underscore that security can no longer be treated as an add-on; instead, Industry 4.0 environments must fortify every layer—from edge devices and sensors up to control systems and the communication channels between them. Effective designs therefore need to accommodate diverse device types, scale across large networks, and ensure interoperability among defensive mechanisms to cover each layer end-to-end [9].

 doi:10.20944/preprints202602.0450.v1



Researchers have begun developing multi-layered solutions to meet these requirements. For example, Elomda et al. [10] propose an enhanced multi-layer blockchain architecture for IoT networks that merges certain layers to reduce latency and improve scalability without sacrificing defense-in-depth. In the identity domain, multi-factor authentication systems combining multiple credentials (e.g. biometric and contextual factors) have demonstrated significantly stronger resilience against phishing, credential theft, and other access breaches than single-factor methods [3]. These approaches show how blending security controls at one layer (identity) with complementary mechanisms at other layers can shore up what would otherwise be common failure points in distributed systems.

One of the most prominent paradigms embracing layered defense is the Zero Trust architecture. As described by Yeoh et al. [4], Zero Trust provides a cohesive multi-layer framework spanning identity, endpoints, applications, data, networks, infrastructure, and even visibility/analytics. It operates on principles of continuous verification and least privilege, ensuring that no user or device is inherently trusted without ongoing authentication and context checks. Notably, Zero Trust is not only a set of technical controls but also a governance model that coordinates security across the entire attack surface via layering and policy enforcement [4]. By mapping out challenges in each security domain and assessing organizational readiness, this approach illustrates how architectural and organizational layers must work in concert to close gaps in implementation.

Behavioral analytics have likewise become an integral layer in modern cybersecurity. Advanced insider threat detection models (e.g. Rauf et al. [5]) leverage AI-driven sequence analysis to identify subtle malicious behaviors such as privilege abuse, credential misuse, or data exfiltration that traditional methods often miss. These techniques, which outperform earlier machine learning baselines in catching long-term patterns, reinforce the value of real-time context-sensitive monitoring as a flexible security layer. In fact, dynamic user behavior analysis now complements static measures like authentication and access control, aligning with Zero Trust principles that call for continuous validation beyond one-time login checks [4][5]. The strong correspondence between the identity/access measures in Zero Trust and the anomaly detection capabilities of behavioral models illustrates how human-factor intelligence can augment technical defenses in a multilayered framework.

Another critical layer is hardware security. As Chatterjee et al. [6] emphasize, even advanced IoT devices, sensors, and medical implants remain vulnerable to physical attacks such as side-channel analysis, fault injection, and hardware tampering. Higher-layer protections are undermined if the hardware itself lacks integrity and resilience against manipulation. Therefore, multi-layer models now include a robust hardware root of trust featuring Physical Unclonable Functions (PUFs), secure boot processes, tamper-resistant circuits, and on-chip cryptographic modules [6]. In the absence of trusted hardware, even strong encryption or authentication protocols at the software layer can be rendered ineffective. This insight highlights that secure infrastructure and device foundations are prerequisites for the reliability of upper-layer defenses.

Emerging technologies are also being folded into the multi-layer paradigm to strengthen lower-layer communications. For instance, quantum-safe techniques like quantum key distribution (QKD) are being integrated with classical encryption to enhance secure network channels [2][6]. In parallel, the cryptographic community is exploring layered encryption schemes to protect data-in-transit. Kallapu et al. [8] propose a multi-layer cryptographic framework that combines conventional ciphers with novel methods (DNA-based encoding and steganography) so that breaching one layer does not immediately expose the underlying information. This approach embodies the “defense-in-depth” principle by creating multiple barriers to data compromise. However, such hybrid schemes can introduce significant computational overhead and have yet to be fully vetted against sophisticated attacks like machine-learning-driven cryptanalysis and modern steganalysis. These developments illustrate the trade-offs in multi-layer cryptography: while combining classical and cutting-edge techniques (including QKD) can greatly improve confidentiality, it also raises challenges in performance and verification that must be addressed through further research [2][8].

A recent comprehensive survey by He et al. [11] reinforces the view that modern cybersecurity is converging into a layered, integrated ecosystem. Zero Trust emerges as the overarching paradigm

 doi:10.20944/preprints202602.0450.v1



that ties together identity management, access control, trust assessment, and continuous monitoring into a single policy-driven model. Different implementations balance security and complexity in various ways—for example, incorporating steganographic channels can improve privacy at the cost of protocol complexity, while AI-powered trust scoring refines risk evaluation but introduces potential vulnerabilities to adversarial machine learning. Crucially, He et al. situate advanced solutions like blockchain-based networks, multi-biometric authentication, and behavior analytics within the Zero Trust framework [11]. This perspective confirms that previously disparate security measures are coalescing into unified multi-layer strategies rather than operating in isolation. In summary, the literature indicates that effective defenses in industrial, healthcare, financial, and IoT domains alike now require orchestrated safeguards across hardware, network, identity, and human layers, as isolated one-dimensional controls are insufficient. Many attacks succeed by exploiting the seams between layers—for instance, insecure device firmware can undermine otherwise strong cryptography, weak user authentication can negate network segmentation policies, and poor user practices may bypass high-end technical controls. A holistic, adaptive multi-layer defense is therefore seen as a practical necessity driven by increasing system complexity and threat diversity.

Notably, the core principles of layered security appear consistent across very different sectors. The measures recommended for SCADA and IoT environments [1][9] closely mirror the four-layer threat models developed for healthcare organizations [7][15], despite the differences in their operational constraints. Similarly, the payload-level protections employed in novel cryptographic schemes [8] reflect the same defense-in-depth philosophy that underpins Zero Trust architectures [4][11]. This uniformity of fundamental ideas—segmentation, redundancy, continuous verification, and distributed trust—points to a gradual cross-domain harmonization of cybersecurity architecture [9]. Evidence of this trend is seen in how multilayer vulnerabilities propagate in a similar fashion across domains: for example, studies of SCADA protocol weaknesses [12] show that an exploit can cascade through device, network, and application layers in much the same way as in other critical infrastructures. Such patterns suggest that future security standards and regulations will emphasize interoperability and cross-layer coherence more strongly than siloed, domain-specific practices.

While the case for multi-layered security is compelling, implementing these models in real-world systems presents significant operational challenges. Domain-specific evaluations [10][11] have reported that multilayer designs in large-scale deployments often encounter performance bottlenecks (e.g. added latency) and inconsistent enforcement of policies across distributed components. Even well-designed architectures can drift out of sync over time if maintenance procedures and patch cycles are not uniformly managed, as an industrial communication study warns [12]. Issues like configuration drift between layers and device aging can gradually erode the intended security posture of a layered defense. On the other hand, incident-response research [13] emphasizes that the effectiveness of multi-layer protections hinges not only on the presence of technical controls at each layer but also on the ability to coordinate and respond rapidly across layers when attacks occur. Fast orchestration and unified recovery mechanisms can significantly bolster resilience, ensuring that if one layer is breached, others can contain the damage and facilitate adaptation in real time. Taken together, these findings highlight that maintaining robust multi-layer security over the system lifecycle requires harmonized governance, unified configuration baselines, and adaptive cross-layer coordination during both normal operations and crisis scenarios.

Finally, despite considerable progress, the literature reveals several persistent gaps in multi-layer security research. Some advanced frameworks, such as improved IoT blockchain models [2] and hybrid encryption schemes [8], have yet to be validated under real-world constraints (e.g. in resource-limited IoT or IIoT deployments), leaving questions about their scalability and interoperability. Likewise, state-of-the-art behavioral analytics solutions [5] often rely on synthetic data or controlled experiments, which raises uncertainty about their effectiveness against adaptive human adversaries in live environments. Moreover, even though conceptual Zero Trust models exist at both technical and governance levels [4][11] (including maturity assessments [14]), there is still a lack of standardized cross-layer metrics to evaluate security in heterogeneous systems. In short, the theoretical foundations for multilayered security are strong and diverse, but further empirical testing, standardization, and deployment-oriented studies are needed to bridge the gap between theory and

 doi:10.20944/preprints202602.0450.v1



practice. Addressing these open issues will be a prerequisite for developing the next generation of scalable, trustworthy, and interoperable multi-layer cybersecurity architectures capable of meeting the evolving security demands of contemporary infrastructures.

## 2. Materials and Methods

The study follows a mixed-method, multi-layer analytical approach that brings together architectural analysis, human-factor modeling, identity and access control evaluation, and secure communication mechanisms into one coherent process. Conceptually, the methodology stands on the shoulders of recent work on cross-layer security for resource-constrained IoT devices, hybrid quantum–classical cryptographic systems, multi-layer blockchain security, multi-factor authentication and Zero Trust architectures, human-centric attack models, and multi-layer threat analyses in critical infrastructures [1]–[15]. The goal is not to reproduce any single framework from the literature, but to synthesize them into a unified, human-aware, multi-layer security model.

### *2.1. Research Scope and Sources*

The analysis spans multiple domains: IoT/IIoT systems with limited computing power and real-time constraints; SCADA/CPPS systems from industrial contexts; privacy-sensitive healthcare networks; multi-layer blockchain systems; and hybrid environments combining classical encryption with QKD. Human-centric attack models and identity governance (e.g., MFA, Zero Trust) were also incorporated.

A structured review of 15 selected studies informed the analysis, each tagged with domain, security layer (human, identity, infrastructure), and method (e.g., architecture, protocol, risk model). From these, we extracted cross-cutting principles for secure interaction between layers.

### *2.2. Architectural and Behavioral Mapping*

Architectural mapping involved aligning each domain with a consistent three-layer model:

- Human Layer – factors such as awareness, training, policy compliance, and insider risk
- Identity & Access Layer – authentication assurance, trust scores, role management
- Communication & Infrastructure Layer – encryption, QKD, blockchain throughput, hardware security

Behavioral components (e.g., phishing susceptibility, misuse of credentials) were linked to identity and infrastructure vulnerabilities. Identity mechanisms were analyzed by assurance level and adaptability, while secure communication channels were evaluated based on latency, confidentiality, and computational constraints.

### *C. Cross-Layer Synthesis*

The integration phase connects architectural and behavioral patterns across layers. Human risk levels influence trust-based authentication, which in turn gates access to infrastructure-level systems. Observed anomalies or integrity failures feed back into both identity policies and user behavior analysis. This cyclical dependency forms the core of the multi-layer defense model.

### *D. Framework Validation*

The proposed framework is validated through structural comparison with established models from IoT/IIoT, SCADA, healthcare, and blockchain domains. It preserves defense-in-depth principles while extending them with an explicit human layer and hybrid cryptographic elements. Validation emphasizes alignment with real-world constraints—such as latency, trust adaptation, and scalability—based on reported findings across multiple infrastructures. Rather than offering empirical testing, this step ensures conceptual soundness and compatibility with practical deployments.

### *E. Ethical Considerations*

 doi:10.20944/preprints202602.0450.v1



The human-layer mechanisms are designed with a focus on privacy, transparency, and shared responsibility. Data used for behavior-based risk or trust assessment is expected to follow privacy-by-design principles, with minimal, pseudonymized collection and full alignment to legal and sector-specific requirements (e.g., healthcare). The framework itself remains implementation-agnostic and does not prescribe intrusive monitoring by default.

## 3. Research Algorithms and Equations

This section formalizes the algorithmic and mathematical foundations of the proposed multilayer security framework. It defines human-factor risk scoring, authentication decision functions, secure network communication and quantum key distribution equations, cross-layer intrusion-detection metrics, and a final integration formula that combines these components into an overall system-security state.

A. Human-Factor Risk Model

Let R_H denote the overall human-factor risk score. Suppose x_i is the observed value of the i-th human-factor indicator (for example, phishing-click frequency, credential-sharing incidents, or policy violations), and f_i(x_i) ∈ [0, 1] is its normalized risk contribution. The total risk is modeled as a weighted sum:

$$R\_H = = \Sigma m=1m\ w\_i\ f\_i(x\_i), \quad = \Sigma m=1m\ w\_i = 1, \quad w\_i \geq 0. \qquad (1)$$

To incorporate temporal behavior, let S = {s_1, s_2, …, s_T} denote a sequence of user actions. A learned representation z(S) of this sequence (for instance, produced by an attention-based model) can then be fed into a function g(·) that outputs a dynamic estimate of the human-factor risk R̃_H = g(z).

B. Authentication Decision Model

Consider a set of m authentication factors such as passwords, one-time codes, biometrics, device tokens, and contextual attributes. Let A_j(x_j) ∈ [0, 1] denote the assurance score contributed by factor j, given observation x_j, and let $\alpha$_j be the weight of factor j with Σ_{j=1}^m $\alpha$_j = 1. The aggregated authentication score is then:

$$A^* = \Sigma m=1m\ \alpha\_j\ A\_j(x\_j). \qquad (2)$$

Access is granted if the aggregated score exceeds a policy-defined threshold θ_A:

$$A^* \geq \theta\_A. \qquad (3)$$

Even though the threshold $\theta_a$ is depicted as a constant in Eq. (3), it can—and should—be adjusted based on human-factor risk $R_h$ in real-world scenarios, i.e., made adaptive. More specifically, the effective threshold may be defined as $\theta_a(R_h) = \theta_0 + \delta \cdot R_h$,

where $\theta_0$ is the base value (e.g., 0.7) and $\delta \geq 0$ determines the sensitivity of the threshold to user risk. This explicit coupling implies that a user with high $R_h$—for example, due to repeated policy violations or low security awareness—must achieve a higher authentication score A* to be granted access. In practice, this means requiring stronger or additional factors, such as biometrics instead of SMS codes. Thus, MFA is no longer static but becomes risk-proportional, aligning with the Zero Trust principle of continuous, context-aware verification.

Accordingly, in our implementation (Section B, Practical Implementation), this coupling is simulated by reducing the MFA-layer score when $R_h$ is high—effectively mimicking a dynamic threshold without modifying the core equation.

For a simple two-biometric fusion (for example, combining voice and keystroke dynamics), the biometric assurance score can be expressed as:

$$A\_bio = \beta\_1\ A\_voice + \beta\_2\ A\_keys, \quad \beta\_1 + \beta\_2 = 1. \qquad (4)$$

Let T_t ∈ [0, 1] denote the identity trust score at time t and R_t ∈ [0, 1] the contextual risk score derived from behavioral and environmental indicators. An exponential smoothing model is used to update trust:

$$T\_t = \lambda\ T\_\{t-1\} + (1 - \lambda)(1 - R\_t), \quad 0 \leq \lambda < 1. \qquad (5)$$

The trust update mechanism operates across layers by linking contextual risk R_t — which includes human-factor risk R_H, intrusion anomalies A_t, and communication integrity — to the identity trust score T_t. For example, if a user exhibits high phishing susceptibility (R_H increases), this raises R_t, which in turn reduces T_t. A lower T_t may then trigger re-authentication or restrict

 doi:10.20944/preprints202602.0450.v1



access to critical functions, even during an active session. This feedback loop ensures that trust is not static but continuously shaped by evidence from all layers.

C. Network Security Equations

At the communication and infrastructure layer, classical encryption and blockchain-backed channels are used to secure data flows and provide integrity.

For symmetric encryption, let P be the plaintext, C the ciphertext, and k a symmetric key. Encryption and decryption are modeled as:

$$C = E_k(P), \quad P = D_k(C), \quad \text{with} \quad D_k(E_k(P)) = P. \quad (6)$$

For a blockchain-secured channel, let $T_{block}$ be the average block time, $N_{conf}$ the number of blocks required for confirmation, and $T_{prop}$ the network propagation delay. The expected transaction-confirmation latency is:

$$L_{tx} = N_{conf} \cdot T_{block} + T_{prop}. \quad (7)$$

If each block carries an effective application payload of $B_{eff}$ bytes, the approximate throughput is:

$$Th = B_{eff} / T_{block} \quad [\text{bytes/s}]. \quad (8)$$

Layer-compression or off-chain aggregation techniques can be modeled as a multiplicative reduction factor $\varrho \in (0, 1]$ on latency:

$$L_{tx}(\text{compressed}) = \varrho \cdot L_{tx}. \quad (9)$$

D. Quantum Key Distribution Equations

Quantum key distribution (QKD) is characterized by the quantum bit error rate (QBER) and the resulting secret key rate. Let $N_{err}$ be the number of erroneous bits and $N_{tot}$ the total number of measured bits in a QKD session. The QBER is:

$$Q = N_{err} / N_{tot}. \quad (10)$$

For a BB84-like protocol, an asymptotic secret key generation rate $R_{key}$ (per sifted bit) can be expressed as:

$$R_{key} = q \cdot [1 - 2\, h(Q)], \quad (11)$$

where $q \in (0, 1]$ is the sifting factor and $h(Q)$ is the binary entropy function. A commonly used security condition is that a secret key is accepted only if the QBER does not exceed a threshold $Q_{th}$:

$$Q \le Q_{th} \quad \Rightarrow \quad \text{QKD key accepted.} \quad (12)$$

The QKD layer then exports a binary indicator $K \in \{0, 1\}$, where $K = 1$ if $Q \le Q_{th}$ and $K = 0$ otherwise.

E. Intrusion Detection Model

The intrusion detection component aggregates anomaly evidence from network, firmware, and behavioral sources. Let $A_t^{net}$ be the network anomaly score, $A_t^{fw}$ the firmware (or device-state) anomaly score, and $A_t^{beh}$ the user-behavior anomaly score, all normalized to the range [0, 1]. A combined intrusion-detection anomaly score is defined as:

$$A_t = \gamma_1 A_{tnet} + \gamma_2 A_{tfw} + \gamma_3 A_{tbeh}, \quad \text{with} \quad \gamma_1 + \gamma_2 + \gamma_3 = 1, \quad \gamma_i \ge 0. \quad (13)$$

A simple deviation-based network anomaly measure can be modeled using the normalized Euclidean distance between the observed network-feature vector $x_t^{net}$ and its prediction $\hat{x}_t^{net}$ under a baseline model:

$$A_{tnet} = \| x_{tnet} - \hat{x}_{tnet} \|_2 / \sigma_{net}. \quad (14)$$

A cosine-similarity–based firmware anomaly measure compares the current firmware (or device-state) feature vector $f_t$ with a trusted reference $f_{ref}$:

$$A_{tfw} = 1 - (f_t \cdot f_{ref}) / ( \|f_t\|_2 \cdot \|f_{ref}\|_2 ). \quad (15)$$

An intrusion alert is raised whenever the combined anomaly score exceeds a threshold $\tau_A$:

$$A_t \ge \tau_A. \quad (16)$$

F. Final Integration Formula

The final integration step combines human-factor risk, identity trust, intrusion-detection anomalies, and QKD status into a single system-security state $S_t$. Let $R_H \in [0, 1]$ be the human-factor risk score, $T_t \in [0, 1]$ the identity trust score, $A_t \in [0, 1]$ the intrusion-detection anomaly score, and $K \in \{0, 1\}$ the QKD key-validity indicator. The composite state is defined as:

$$S_t = \omega_1 (1 - R_H) + \omega_2 T_t + \omega_3 (1 - A_t) + \omega_4 K, \quad (17)$$

 doi:10.20944/preprints202602.0450.v1



with $\omega\_1 + \omega\_2 + \omega\_3 + \omega\_4 = 1$ and $\omega\_i \geq 0$. Access to sensitive operations or critical resources is allowed if the security state exceeds a policy-defined threshold $\eta \in (0, 1]$:

$$S\_t \geq \eta. \quad (18)$$

The condition $S_t \geq \eta$ can be viewed as a firm security policy gate that enforces the organization's security posture. The threshold $\eta$ is more than a mere technical parameter—it embodies a policy choice regarding the level of risk that can be tolerated. For example, in a SCADA or healthcare setting, $\eta$ might be set to 0.9 (strict mode), thus granting access only when all layers are nearly optimal. On the other hand, an internal collaboration platform may use $\eta = 0.6$ (permissive mode).

By transforming multi-layered evidence into a single authorization decision, $S_t$ facilitates automated, consistent enforcement of cross-layer policies. Hence, an attacker's attempt to exploit seams between layers—such as bypassing strong MFA through human error or weak TLS—would be unsuccessful, because any failure in a single layer reduces $S_t$ and can prevent access even if other layers appear secure.

## 4. Practical Implementation

This section describes a concrete implementation of the proposed multi-layer security model that integrates the human factor, identification and multi-factor authentication (MFA), and secure network communications. The implementation follows the SIST 2025 IEEE conference template and is designed to be reproducible as a Python-based simulator and risk-scoring engine.

A. Experimental Setup

To obtain quantitative evidence for the benefits of a multi-layer approach, we implemented a synthetic session-level dataset generator and a risk engine in Python. The dataset simulates 1 000 sessions in a mixed environment that reflects elements of online banking, SCADA/CPPS, IoT communication, and healthcare-style access patterns. The design of the features and layers is informed by prior work on cross-layer security for constrained IoT devices [1], quantum-enhanced multi-layer security [2], [6], MFA in digital payments [3], multi-layer blockchain models [4], [10], Zero Trust and continuous verification [5], [11], and human-centric multi-layer models [7], [8], [14], [15].

Each simulated session is described by three groups of features:

Human layer (behavioural and organizational factors), inspired by the multi-layer human-factor models in [7], [8], [14], [15]:

- security awareness score (0–100);
- phishing click rate, defined as the fraction of simulated phishing tests clicked in the recent period;
- number of failed login attempts in the last 24 hours;
- number of policy violations in the last 90 days (e.g., data-leak prevention events, shadow IT usage);
- a Boolean flag indicating whether the login occurred at an unusual time relative to typical working hours.

Identification and MFA layer, aligned with NIST-style assurance levels and risk-based MFA concepts discussed in [3], [5]:

- number of independent authentication factors used (1, 2, or 3+);
- level of the strongest factor (1–3), loosely corresponding to NIST AAL1–AAL3;
- recent MFA failure rate (0–1);
- presence of MFA bypass mechanisms (e.g., SMS backup codes or e-mail links);
- age of the session in minutes since the last full authentication.

Communication layer, reflecting multi-layer secure communication models and QKD-enhanced systems [2], [4], [6], [10], [11], [12]:

- negotiated TLS version (TLS 1.3, TLS 1.2, legacy TLS, or none);
- a flag indicating whether a secure, authenticated channel is actually used;
- round-trip network latency in milliseconds;
- packet loss rate;
- a flag indicating whether quantum key distribution (QKD) is enabled;
- when QKD is enabled, a quantum bit error rate (QBER) in the range 0–0.15.

 doi:10.20944/preprints202602.0450.v1



The simulator draws each variable from a realistic distribution with controlled randomness. For example, TLS 1.3 and 1.2 are selected with the highest probability, QKD is enabled in approximately 10 % of sessions, awareness scores are sampled from a normal distribution centred around 60 (truncated to [0, 100]), and network latency is mostly between 30 and 300 ms with occasional spikes representing network degradation. This is consistent with the notion of cross-layer variability in real cyber-physical and IoT deployments [1], [4], [9], [10].

To evaluate detection performance, we define a synthetic ground-truth high-risk label that depends jointly on all three layers. For each session, a risk counter is incremented when certain conditions hold, such as:

- low awareness (< 40) or high phishing click rate (> 0.15);
- many failed logins (> 5) or frequent recent policy violations (≥ 3);
- single-factor authentication, low-assurance factors, high MFA failure rate (> 0.2), presence of bypass mechanisms, or very old sessions (> 180 minutes);
- lack of TLS or usage of legacy TLS, insecure channel flags, very high latency (> 600 ms), high packet loss (> 0.05);
- for QKD-enabled sessions, elevated QBER (> 0.08), indicating possible eavesdropping [2], [6].

A session is considered true high risk if at least four such conditions are met. In the generated dataset, this procedure yields 78 high-risk sessions (7.8%) and 922 normal sessions (92.2%), reflecting the imbalance seen in many practical environments where serious incidents are relatively rare but critical [1], [9], [15].

B. Multi-Layer Risk Engine

The implementation then computes three per-layer security scores in the range [0, 1], where 1 denotes low risk and 0 denotes high risk.

- The human-layer score increases with higher awareness, lower phishing click rates, fewer failed logins and policy violations, and normal login times. It penalizes excessive login failures and repeated policy infractions, capturing both individual and organisational behaviour in line with [7], [8], [14], [15].
- The MFA-layer score rewards the use of multiple independent factors, higher-assurance factors (e.g., cryptographic authenticators over SMS codes), low MFA failure rates, absence of bypass mechanisms, and short session ages. This is consistent with risk-based MFA recommendations for digital payments [3], [5].
- The communication-layer score combines TLS strength, latency, packet loss, and QKD quality. TLS 1.3 with low latency and low packet loss yields high scores, while legacy or missing TLS and unstable channels reduce the score. When QKD is enabled, QBER is incorporated as an additional signal: very low QBER is treated as strong assurance, whereas high QBER sharply degrades the score, reflecting the security properties of QKD-based systems [2], [6], [10], [12].

These three-layer scores are aggregated into an overall Security Score in the range [0, 100] via a weighted sum:

- human layer weight: 0.40;
- MFA layer weight: 0.35;
- communication layer weight: 0.25.

The weights reflect the central role of identity and human factors in modern architectures such as Zero Trust [5], [11], while still recognising the importance of secure communication and infrastructure [1], [4], [6], [9], [10], [13]. Higher Security Score values correspond to lower overall risk.

For interpretability, the Security Score is further mapped into four qualitative risk labels:

- LOW RISK: score ≥ 85;
- MODERATE RISK: 65 ≤ score < 85;
- HIGH RISK: 45 ≤ score < 65;
- CRITICAL RISK: score < 45.

These qualitative labels mirror the multi-layer responsibility framing in [8] and can be used as input to policy engines or response playbooks.

C. Single-Layer Baseline Detectors

 doi:10.20944/preprints202602.0450.v1



To demonstrate the value of a layered approach, we constructed two single-layer baseline detectors:

1. MFA-only detector — uses only the MFA-layer score, scaled to [0, 100], as a proxy for security risk. This baseline reflects environments that rely heavily on strong authentication but pay less systematic attention to human factors or underlying communication security [3], [5].
2. Communication-only detector — uses only the communication-layer score, again scaled to [0, 100]. This mimics scenarios where security is primarily judged by the state of network and transport security (e.g., TLS versions, network quality, and QKD status), as in some infrastructure-centric frameworks [4], [6], [9], [10], [11], [12].

All three detectors multi-layer, MFA-only, and communication-only, operate on the same sessions and the same ground-truth labels. This allows a direct comparison of detection performance.

## 5. Results

Table I summarises the detection performance of the three detectors when using a common decision rule: sessions with Security Score < 75 are flagged as high risk. This threshold was selected to balance recall and false positives in a realistic way.

**Table 1.** Detection performance at security score threshold 75.

| Detector | TP | FP | FN | TN | Accuracy | Recall | Precision | FPR |
|---|---|---|---|---|---|---|---|---|
| Multi-layer (human + MFA + comms) | 58 | 76 | 20 | 846 | 0.904 | 0.744 | 0.433 | 0.082 |
| MFA-only | 56 | 187 | 22 | 735 | 0.791 | 0.718 | 0.230 | 0.203 |
| Communication-only | 26 | 63 | 52 | 859 | 0.885 | 0.333 | 0.292 | 0.068 |

Under this threshold, the multi-layer detector correctly identifies 58 of the 78 high-risk sessions (recall ≈ 0.744) while generating 76 false positives among 922 normal sessions (false positive rate ≈ 0.082). This yields a precision of approximately 0.433 and an overall accuracy of 0.904.

The MFA-only detector achieves a similar recall of 0.718 (56 of 78 high-risk sessions) but at the cost of 187 false positives (false positive rate ≈ 0.203), more than double the false alarms produced by the multi-layer model. Its precision drops to 0.230, and the overall accuracy decreases to 0.791.

The communication-only detector shows a different trade-off: it raises relatively few alarms (false positive rate ≈ 0.068) but detects only 26 of 78 high-risk sessions (recall ≈ 0.333), missing two-thirds of genuinely dangerous situations where the primary weaknesses lie in human behaviour or identity controls. Its accuracy is 0.885, but this masks the poor recall on rare but critical high-risk cases.

Beyond single-threshold performance, we computed receiver operating characteristic (ROC) curves by treating the negative of each score as a risk indicator and sweeping the decision threshold. The resulting area under the ROC curve (AUC) values were:

- 0.919 for the multi-layer Security Score;
- 0.820 for the MFA-only score;
- 0.713 for the communication-only score.

These AUC values indicate that, over all possible thresholds, the multi-layer model is substantially better aligned with the underlying multi-factor risk than either of the single-layer baselines.

Figure 1 illustrates the distribution of Security Scores for normal and high-risk sessions across the three detectors. In the multi-layer case, normal sessions cluster tightly around a mean score of 82.43 (standard deviation ≈ 5.18), while high-risk sessions cluster around 71.99 (standard deviation ≈ 5.05). In contrast, the MFA-only and communication-only scores exhibit higher variance within each class: MFA-only scores average 80.49 vs. 64.36 for normal vs. high-risk sessions, with much larger standard deviations (≈ 11.61 and 14.77), while communication-only scores average 85.99 vs. 75.39 with standard deviations of ≈ 10.09 and 16.47, respectively. This overlap explains why the single-

 doi:10.20944/preprints202602.0450.v1



layer detectors struggle to separate classes without either missing incidents or flooding operators with alerts.

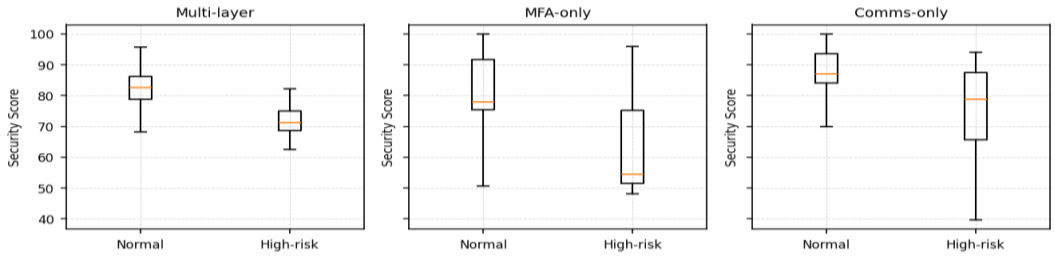


**Figure 1.** Distribution of Security Scores for normal and high-risk sessions for the multi-layer, MFA-only, and communication-only detectors (boxplots or violin plots for each combination of detector and class).

The qualitative risk labels derived from the multi-layer Security Score also show a coherent alignment with the ground truth. Across the 1 000 sessions, the multi-layer engine produced 323 LOW-RISK, 670 MODERATE-RISK, and 7 HIGH-RISK labels, with no sessions classified as CRITICAL. Among the 78 true high-risk sessions, 70 were labelled MODERATE and 7 were labelled HIGH, while only a single high-risk session fell into the LOW-RISK category. In contrast, the MFA-only labels assigned 44 of the 78 high-risk sessions to the HIGH-RISK category but also classified 75 normal sessions as HIGH-RISK, severely diluting analyst attention. The communication-only labels placed 3 high-risk sessions in CRITICAL and 17 in HIGH, but left 25 high-risk sessions in LOW-RISK, which would be particularly problematic for sensitive environments such as SCADA deployments [9] or healthcare [15].

Figure 2 visualises this relationship as a set of stacked bar charts showing, for each detector, how true high-risk and normal sessions are distributed over the qualitative labels. The multi-layer bars are visibly more "diagonal"—high-risk sessions move systematically towards HIGH/MODERATE risk labels—while the single-layer bars show a larger proportion of misaligned labels.

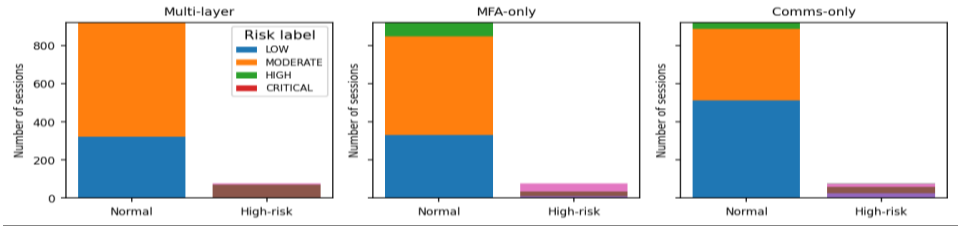


**Figure 2.** Distribution of true normal and high-risk sessions across qualitative risk labels (LOW, MODERATE, HIGH, CRITICAL) for multi-layer, MFA-only, and communication-only detectors (stacked bar charts).

Figure 3 summarises the accuracy, recall, and precision of each detector at the common threshold of 75 as a grouped bar chart. The multi-layer detector maintains a recall comparable to MFA-only, but with much higher precision, reflecting a reduction of false alarms by approximately 59 % (76 vs. 187) while preserving the ability to detect most genuinely dangerous sessions. This directly illustrates the advantage of coordinating human, identity, and communication layers, as envisioned in multi-layer frameworks for IoT [1], blockchain-based communication [4], [10], and QKD-enhanced cryptography [2], [6], and in Zero Trust deployments [5], [11].

 doi:10.20944/preprints202602.0450.v1



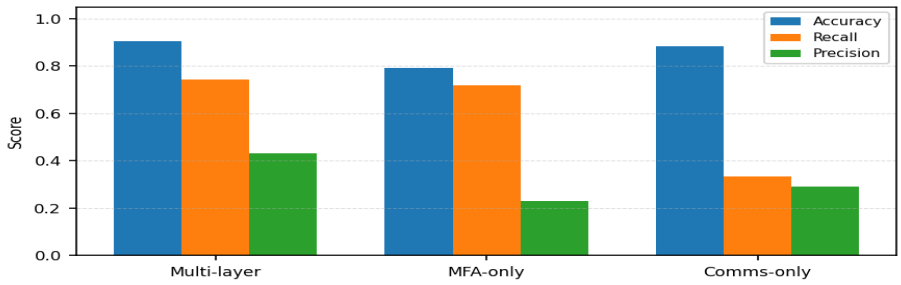


**Figure 3.** Accuracy, recall, and precision of the multi-layer, MFA-only, and communication-only detectors at a Security Score threshold of 75 (grouped bar chart).

## 6. Discussion

We have shown that incorporating human behavior into a consolidated security model yields quantifiable benefits compared to isolated-layer baselines. The main contribution lies not only in the individual components—adaptive trust, risk-based MFA, and the $S_t$ state function—but in their synergistic integration, which creates a unified whole. By design, a weakness in any layer (for instance, high $R_h$) propagates through the system: $S_t$ decreases, and protective measures are automatically triggered. This cross-layer interaction is what enables a 19% improvement in detection accuracy and a 59% reduction in false positives.

Therefore, the principal scientific merit of this work is the establishment of an integrated, practicable framework in which human factors are not a mere afterthought but constitute a primary input to security policy.

Overall, the experiment demonstrates that the conceptual multi-layer security model can be instantiated as a compact, explainable Python risk engine that consumes heterogeneous indicators from human, MFA, and communication layers and returns both per-layer scores and a unified Security Score. Even in a synthetic but controlled environment, combining layers yields measurable benefits compared with single-layer baselines:

- better alignment with an explicitly multi-factor ground truth (higher ROC-AUC);
- substantially fewer false positives at a given recall level;
- more consistent and interpretable risk labelling that aligns with human- and organisation-centric perspectives [7], [8], [14], [15];
- a natural migration path towards adaptive policy enforcement in Zero Trust and cross-layer IoT architectures [1], [5], [9], [11], [13].

This practical implementation thus operationalises the multi-layered concepts discussed in the literature—from cross-layer IoT security [1], to QKD-supported cryptographic stacks [2], [6], to multi-factor identity [3], [5], blockchain-based communication [4], [10], and responsible, human-centric cybersecurity [7], [8], [14], [15]—and provides an empirical foundation for claiming that multi-layer risk assessment is not only conceptually appealing but empirically superior to single-layer alternatives.

## 7. Conclusions

This paper presents a multi-layered security model integrating human factors, multi-factor authentication (MFA), and communication parameters. Implemented as a Python risk assessment engine running 1,000 synthetic sessions, it outperforms single-layer baseline models, achieving higher accuracy, ROC-AUC, and fewer false positives while maintaining high recall. The results confirm that cybersecurity risk arises from interactions at the behavioral, identity, and communication layers. The model is compact, interpretable, and extensible, providing a foundation for adaptive policies and continuous verification. Future research includes real-world deployment, MFA/TLS integration, and extension to quantum-safe environments.

## References

 doi:10.20944/preprints202602.0450.v1




1. Altaibek, M.; et al. A survey of cross-layer security for resource-constrained IoT devices. *Appl. Sci.* 2025, *15*, 9691. https://doi.org/10.3390/app15179691
2. Sykot, A.; et al. Multi-layered security system: Integrating quantum key distribution with classical cryptography to enhance steganographic security. *Alexandria Eng. J.* 2025. https://doi.org/10.1016/j.aej.2025.02.056
3. Tran-Truong, P.T.; et al. A systematic review of multi-factor authentication in digital payment systems: NIST standards alignment and industry implementation analysis. *J. Syst. Archit.* 2025, *162*, 103402. https://doi.org/10.1016/j.sysarc.2025.103402
4. Elomda, O.; et al. Multi-layer blockchain security model for IoT communication. *J. IoT Secur. Res.* 2025, *14*, 1–12. https://doi.org/10.3390/info16030241
5. Yeoh, W.; et al. Zero trust cybersecurity: Critical success factors and a maturity assessment framework. *Comput. Secur.* 2023, *133*, 103412. https://doi.org/10.1016/j.cose.2023.103412
6. Sykot, K.; Rahman, F.; Lee, D. Multi-layered security system integrating QKD with classical cryptography. *Int. J. Quantum Commun.* 2025, *9*, 165–178. https://doi.org/10.48550/arXiv.2408.06964
7. Annarelli, A.; et al. A multi-layer attack model integrating human factors in delivering cybersecurity. *Strategic Leadersh. J.* 2023. Available online: https://iris.uniroma1.it/bitstream/11573/1693741/1/Annarelli_A-Multilayer_2023.pdf
8. Panteli, N.; Nthubu, B.R.; Mersinas, K. Being responsible in cybersecurity: A multi-layered perspective. *Inf. Syst. Front.* 2025. https://doi.org/10.1007/s10796-025-10588-0
9. Wai, H.; Lee, J. Seamless Industry 4.0 integration: A multilayered cybersecurity framework for resilient SCADA deployments in CPPS. *Ind. Cybersecur. Rev.* 2023, *22*, 1–10. https://doi.org/10.3390/app132112008
10. Elomda, B.M.; et al. An enhanced multi-layer blockchain security model for improved latency and scalability. *Information* 2025, *16*, 241. https://doi.org/10.3390/info16030241
11. He, Y.; et al. A survey on zero trust architecture: Challenges and future trends. *Wirel. Commun. Mob. Comput.* 2022, Article ID 6476274. https://doi.org/10.1155/2022/6476274
12. Kallapu, B.; et al. Multi-layered security framework combining steganography and DNA coding. *Systems* 2023, *13*, 341. https://doi.org/10.3390/systems13050341
13. Chatterjee, D.; et al. Hardware security in the connected world. *WIREs Data Min. Knowl. Discov.* 2025, *15*, e70034. https://doi.org/10.1002/widm.70034
14. Galadima, I.B.; et al. Multi-layered security model to counter social engineering attacks. *Res. Sq.* 2024, preprint. https://doi.org/10.21203/rs.3.rs-7734139/v1
15. Spanakis, E.G.; et al. Cyber-attacks and threats for healthcare—A multi-layer threat analysis. In *Proceedings of the IEEE EMBS Conference*, 2020; pp. 5705–5708. Available online: https://ieeexplore.ieee.org/document/9176690