ISSN: 2583-7354

International Journal of Emerging Knowledge Studies

Publisher's Home Page: https://www.ijeks.com/

Fully Open Access Research Paper

Quantum-Resilient Hybrid Encryption Framework with Behavioural Biometrics for Enhanced Multi-Layer Cloud Authentication

Dr. J. Mohammed Ubada[1*]

[1]PG & Research Department of Computer Science, Jamal Mohamed College (Affiliated to Bharathidasan University), Trichy, Tamil Nadu, India.

DOI: https://doi.org/10.70333/ijeks-05-07-008

*Corresponding Author: ubada786@gmail.com

Article Info: - Received : 19 May 2026 **Accepted** : 25 June 2026 **Published** : 30 June 2026

Abstract

This work proposes a quantum-resilient hybrid encryption framework that combines classical and post-quantum cryptographic mechanisms with behavioural biometrics to strengthen multi-layer cloud authentication. The framework is designed to address the weakness of static credentials by adding continuous identity verification based on user behaviour such as typing rhythm, mouse dynamics, and interaction patterns, which are well suited for adaptive cloud security. By integrating hybrid cryptography, the model aims to preserve confidentiality and interoperability during the transition to post-quantum security while reducing the risk posed by future quantum adversaries. The overall contribution is a layered authentication approach that improves resilience, supports continuous verification, and balances security with usability in cloud environments.

Keywords: *Quantum-Resilient Security, Hybrid Encryption, Behavioural Biometrics, Cloud Authentication, Post-Quantum Cryptography, Continuous Authentication, Multi-Layer Security.*

1. Introduction

This study addresses the growing need for secure authentication in cloud environments where both classical cyberattacks and future quantum threats must be considered. Traditional login-based systems are often vulnerable to password theft, phishing, session hijacking, and replay attacks, while emerging quantum computing capabilities may weaken widely used public-key cryptographic methods [1]. To respond to these risks, the proposed framework combines quantum-resilient hybrid encryption with behavioural biometrics to create a stronger and more adaptive authentication model. The main idea is to support both secure data protection and continuous user verification, so that trust is not

established only at login but maintained throughout the session.

The motivation for this work comes from the increasing complexity of cloud access, where users often connect from multiple devices, networks, and locations. In such settings, static credentials are not sufficient because attackers may gain access through stolen passwords or compromised tokens [2]. Behavioural biometrics such as typing rhythm, mouse movement, and interaction patterns can help verify whether the current user is the legitimate account holder. By integrating these behavioural signals with post-quantum hybrid encryption, the framework aims to deliver better security, stronger resilience, and improved usability for modern cloud systems.

1.1. Background and Motivation

The rapid growth of cloud computing has increased dependence on centralized identity and access management, making authentication a critical security layer for protecting sensitive data and services. At the same time, classical public-key cryptosystems face increasing long-term risk from quantum computing, which has accelerated interest in post-quantum cryptography and hybrid migration strategies [3]. In parallel, behavioural biometrics has emerged as a practical way to support continuous authentication because it can observe user actions in real time rather than relying only on passwords or one-time login checks. These three trends together motivate a framework that is not only quantum-resistant but also adaptive to cloud usage patterns and user behaviour.

1.2. Problem Statement

Current cloud authentication systems often rely on static credentials, traditional MFA, or isolated security layers that do not fully address advanced threats such as credential theft, session hijacking, insider misuse, or future quantum attacks. Traditional authentication also tends to stop at login, leaving active sessions exposed when user context changes or when an attacker gains partial access [4]. Moreover, many systems that add extra security layers do so without integrating cryptographic resilience and behavioural verification into one coherent architecture. The problem, therefore, is how to design a cloud authentication framework that remains secure against quantum-era risks while continuously validating the user in a low-friction way.

1.3. Objectives and contributions

The main objective of this work is to develop a layered authentication framework that combines hybrid encryption with behavioural biometric verification for cloud environments. A second objective is to ensure that the framework remains compatible with current infrastructure while providing a practical transition path toward post-quantum security [5]. The contribution is a model that links cryptographic protection, continuous identity assurance, and adaptive authentication decisions into a single architecture. This integrated approach is intended to reduce attack surface, improve resistance to impersonation, and maintain usability during cloud access and ongoing session activity.

1.4. Scope of the Work

This work focuses on multi-layer cloud authentication, with emphasis on hybrid encryption, behavioural biometric monitoring, and secure session handling. It covers the design of authentication flows, selection of cryptographic primitives, biometric feature usage, and the security rationale for combining these components [6]. The scope does not attempt to replace all enterprise identity systems; instead, it proposes an enhancement layer that can integrate with existing IAM and cloud access workflows. The discussion also considers implementation feasibility, privacy concerns, and the trade-off between stronger security and user convenience.

2. Related Work and Literature Review

Research in this area spans three major domains: post-quantum cryptography, hybrid encryption, and behavioural biometrics. Post-quantum cryptography has developed rapidly in response to the threat that quantum computers pose to classical public-key algorithms [7]. Hybrid encryption frameworks have emerged as a practical migration strategy, allowing systems to use both established and quantum-safe primitives during a transition period. Behavioural biometrics has meanwhile

gained attention as a continuous authentication technique that can improve account protection after login.

2.1. Post-quantum Cryptography Overview

Post-quantum cryptography has become a major research and standardization area because quantum computers threaten widely used public-key algorithms. The literature shows strong attention on lattice-based, hash-based, code-based, isogeny-based, and multivariate schemes, with lattice-based methods receiving particularly strong practical interest for encryption and key exchange [8]. Recent work also emphasizes deployment issues such as implementation efficiency, side-channel resistance, and compatibility with existing systems. For a cloud authentication framework, this body of research is important because key establishment and secure communication must remain trustworthy even under future quantum capabilities.

2.2. Hybrid Encryption Frameworks

Hybrid encryption frameworks combine classical cryptography with post-quantum techniques to preserve interoperability while improving resistance to quantum attacks. The literature describes layered, composite, and interoperable hybrid patterns, each balancing migration ease, performance, and security differently [9]. Recent reviews also argue that hybrid approaches are often the most realistic near-term option because they allow systems to keep operating while gradually introducing quantum-safe primitives. In cloud settings, hybrid encryption is especially valuable because authentication traffic, session keys, and stored secrets often pass through multiple trust domains.

2.3 Behavioural Biometrics in Authentication

Behavioural biometrics uses patterns such as keystroke dynamics, mouse movement, touch behaviour, and interaction timing to recognize users continuously. Research in this area shows that such signals can support passive authentication, meaning the system can verify identity without repeatedly interrupting the user [10]. The literature also notes that behavioural data is useful against attacks that bypass static authentication, including credential stuffing, session misuse, and account takeover. However, studies also highlight challenges such as behavioural drift, noisy measurements, spoofing attempts, and the need for careful threshold tuning.

2.4. Multi-layer Cloud Authentication Models

Multi-layer cloud authentication models typically combine identity checks across device, user, session, and contextual layers to improve assurance. These models are often built around risk-based authentication or zero-trust ideas, where trust is continuously reassessed rather than granted once at login [11]. Recent adaptive cloud authentication studies show that integrating behavioural biometrics with contextual signals can reduce compromise without significantly harming user productivity. This supports the idea that a layered framework is more resilient than a single-factor or one-time authentication process, especially in enterprise cloud environments.

2.5. Research Gaps

Although the literature separately advances post-quantum cryptography, hybrid encryption, and behavioural biometrics, fewer works integrate all three into one cloud authentication framework. A key gap is the lack of designs that connect quantum-resilient key management with continuous behavioural verification in a coordinated protocol [12]. Another gap is limited practical guidance on how to preserve usability and privacy while binding biometric signals to authentication decisions. This creates room for a framework that treats cryptographic resilience, behavioural identity, and cloud-layer orchestration as mutually supporting components rather than isolated controls.

3. System Requirements and Threat Model

This section defines the operational, security, privacy, and usability expectations of the proposed authentication framework. A cloud authentication system must do more than verify a user once; it must remain reliable under changing contexts, multiple devices, and evolving attack methods [13]. The framework therefore needs to satisfy functional goals such as secure login, continuous verification, session control, and revocation, while also resisting

credential theft and adversarial manipulation. A practical design must also consider privacy regulations, low-friction user experience, and deployment constraints in multi-cloud environments. The threat model clarifies what kinds of attackers are assumed, what assets are protected, and where the boundaries of trust lie [14]. In formal terms, the overall security objective can be expressed as minimizing the probability of unauthorized access P_{ua}while preserving legitimate access quality P_{la}, ideally achieving $P_{ua} \to 0$and $P_{la} \to 1$under realistic system conditions.

3.1. Functional Requirements

The functional requirements describe what the system must do in order to support secure and usable cloud authentication. At a minimum, the framework must support user enrolment, initial authentication, continuous session validation, session termination, and credential or template revocation [15]. It must also integrate behavioural biometrics and hybrid encryption without disrupting normal cloud operations. Since cloud environments often involve distributed services, the system should operate across devices, gateways, and backend identity services while maintaining consistent policy enforcement. Another important requirement is adaptability: the framework should be able to increase verification intensity when risk is high and reduce friction during normal use. A simple way to represent the functional decision process is $A = f(C, B, R)$, where $A$is the authentication outcome, $C$is cryptographic verification, $B$is behavioral evidence, and $R$is contextual risk [16]. This ensures the system responds dynamically rather than relying on a single static login event.

3.2. Security Requirements

Security requirements define the protection goals the framework must satisfy against both present-day and quantum-era threats. The system must ensure confidentiality, integrity, authentication, non-repudiation where needed, and resistance to replay, impersonation, and session hijacking [17]. Because the design includes hybrid encryption, the cryptographic layer should remain secure even if one component becomes weaker over time. Behavioural authentication must also be protected from spoofing, adversarial manipulation, and template theft. A strong design should enforce key freshness and forward secrecy, especially for session establishment. In abstract terms, the system should maintain secrecy probability Sclose to 1 and compromise probability Cclose to 0, with the relationship $C = 1 - S$. For example, if a session key is derived through secure hybrid exchange, then the compromise of one mechanism should not automatically expose the full session [18]. This layered security principle is especially important for cloud systems where attackers may target endpoints, networks, or stored authentication artifacts.

3.3. Privacy Requirements

Privacy requirements ensure that user data, especially behavioural biometric data, is handled in a way that minimizes exposure and misuse [19]. Unlike passwords, behavioural biometrics cannot simply be changed if leaked, so the framework must apply stronger protection to templates, feature vectors, and metadata. The system should follow data minimization, purpose limitation, secure storage, and limited retention principles. It should avoid unnecessary collection of raw biometric traces when derived features are sufficient. Template protection methods such as hashing, transformation, cancellable biometrics, or secure storage in trusted modules should be considered. A useful privacy metric is information leakage L, which should be minimized as much as possible, while utility Ushould remain high: $\min L$subject to $U \geq U_{min}$. The challenge is to preserve enough biometric signal for reliable authentication while preventing reconstruction of original behavioral patterns [20]. This is especially important in cloud settings where data may traverse multiple services, regions, and administrative domains.

3.4. Usability Requirements

Usability requirements focus on making the security model practical for everyday users. A system that is too slow, intrusive, or unstable will not be adopted, even if it is technically strong [21]. Therefore, the proposed framework should reduce repeated login prompts, avoid excessive verification steps, and handle normal behavioural variation without generating too

many false alarms. The authentication process should be smooth enough for routine use while still reacting to suspicious behaviour. Usability can be described as a function $U = g(T, E, F)$, where $T$is time cost, $E$is user effort, and $F$is friction introduced by security checks. In general, the goal is to minimize T, E, and F while keeping assurance high. This is why continuous authentication is useful it can validate identity passively in the background rather than interrupting the user repeatedly [22]. The framework should therefore balance strong security with low interaction cost.

3.5. Threat Model and Adversary Assumptions

The threat model defines the likely attackers and the attack surfaces they may exploit. The framework should assume external attackers who attempt phishing, replay, credential stuffing, malware-based theft, man-in-the-middle interception, and session hijacking. It should also assume insider threats, compromised endpoints, and adversaries with partial access to logs or metadata [23]. In a future-oriented view, the model should include quantum-capable adversaries that may eventually weaken classical public-key protection. The attacker's success can be modelled as a probability P_{succ}, which depends on access level, computational power, and available stolen data. A secure design aims to reduce P_{succ}across all realistic attack paths. The framework should also assume that behavioral data may be noisy, incomplete, or occasionally spoofed, so decisions must account for uncertainty rather than relying on perfect observations. This makes layered authentication and risk-based policy essential.

4. Proposed Framework Architecture

The proposed architecture organizes authentication into multiple coordinated layers so that encryption, behavioural verification, and session control work together. A layered design is important because cloud systems are distributed and expose multiple points of failure, including clients, APIs, gateways, identity providers, and backend services [24]. The architecture should therefore separate trust-sensitive functions and ensure that each layer contributes to the final access decision. The framework can be understood as a pipeline in which the user first proves cryptographic legitimacy, then behavioural consistency, and finally ongoing session trust [25]. The overall architecture should also support adaptive policy decisions based on context, risk, and confidence scores. Mathematically, the system trust score may be represented as

$$T = \alpha C + \beta B + \gamma X \quad (1)$$

where $C$is cryptographic confidence, $B$is biometric confidence, $X$is contextual evidence, and

$$\alpha + \beta + \gamma = 1 \quad (2)$$

This allows the system to combine evidence rather than relying on any single signal.

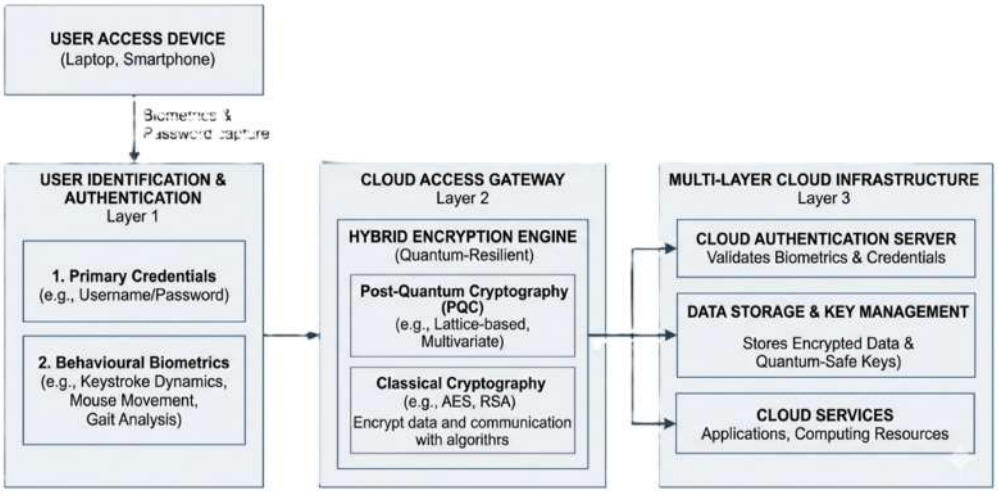

Figure-1. Quantum-Resilient Hybrid Encryption Framework

4.1. Overall System Architecture

The overall system architecture consists of client devices, a secure access gateway, an authentication engine, a biometric analysis module, a key management service, and cloud application endpoints. The client gathers behavioural signals and participates in cryptographic handshakes, while the gateway coordinates authentication requests and policy checks [26]. The backend verifies keys, evaluates biometric confidence, and issues session tokens or access grants. This separation improves modularity and makes the framework easier to deploy in existing cloud environments. A typical flow begins when the client submits credentials and cryptographic proofs, followed by biometric verification and then session establishment. If the architecture is designed properly, the probability of unauthorized entry becomes the product of multiple independent failures, approximately

$$P_{unau} = P_1 \times P_2 \times P_3 \quad (3)$$

where each term represents one protection layer [27]. This layered multiplication is the key advantage of the framework, because an attacker must defeat several controls at once.

4.2. Cloud Authentication Layers

The cloud authentication layers represent distinct checkpoints where identity and trust are evaluated. The first layer typically verifies the initial cryptographic identity of the user or device. The second layer checks behavioural consistency and contextual signals such as device posture, location, or session history [28]. The third layer performs continuous monitoring after login, allowing the system to react if behaviour deviates from the expected pattern. This structure is especially suitable for cloud systems because access is often long-lived and distributed across services. The authentication strength can be modelled as

$$S_{total} = 1 - \prod_{i=1}^{n}(1 - s_i) \quad (4)$$

where $s_i$is the security contribution of each layer. As the number of effective layers increases, the overall assurance improves [29]. However, these layers must be coordinated carefully to avoid redundant checks or contradictory decisions. The design should therefore make each layer complementary, not isolated.

4.3. Client-side and server-side components

The client-side components include biometric capture modules, secure storage for local secrets, cryptographic libraries, and session monitoring functions. The server-side components include the authentication engine, policy decision point, biometric matching support, key management, audit logging, and token issuance services [30]. Client-side processing is useful because it can reduce exposure of sensitive behavioural data and support local trust decisions before data is transmitted. Server-side processing, on the other hand, centralizes policy enforcement and enables global visibility across cloud services. A clean split between these components improves security and performance. The security of the system can be represented as

$$G = f(g_c, g_s) \quad (5)$$

where $g_c$is client trust and $g_s$is server trust. If either side is weak, the overall defense is weakened. For this reason, the architecture should avoid placing all trust in one endpoint or one control plane.

4.4. Data Flow and Control Flow

Data flow describes how authentication information moves through the system, while control flow describes how decisions are made in response to that data. The data flow usually begins with biometric capture and cryptographic initialization on the client, followed by secure transmission to the cloud authentication service [31]. The control flow processes the evidence, computes confidence scores, and determines whether access should be granted, limited, or denied. During the session, additional behavioural observations may trigger re-authentication or revocation. A simple decision rule may be written as

$$D = \mathbb{1}(w_b B + w_c C + w_r R \geq \theta) \quad (6)$$

where $D$is the access decision, $B$is biometric score, $C$is cryptographic validation, $R$is risk, and $\theta$is the threshold. This structure is

useful because it makes the policy logic explicit and tunable [32]. Proper design of data and control flow is essential to avoid bottlenecks and to ensure timely reactions to suspicious activity.

4.5. Trust Boundaries

Trust boundaries define where the system must stop assuming security and begin verifying it. In cloud authentication, trust boundaries usually exist between user devices, local networks, gateways, cloud services, and third-party infrastructure [33]. The framework must treat each boundary as potentially hostile unless proven otherwise. This is especially important when behavioural data, keys, or session tokens move across services. Clearly defining trust boundaries helps determine where encryption is required, where validation should occur, and where sensitive data should never be exposed in raw form. The number of trust boundary crossings can be approximated as N_{tb}, and the attack exposure generally increases with N_{tb}, so the design should reduce unnecessary crossings whenever possible [34]. Boundaries also help identify which component is responsible if an incident occurs. In practical terms, this supports auditing, segmentation, and least-privilege access control.

5. Quantum-Resilient Hybrid Encryption Design

The quantum-resilient hybrid encryption design aims to protect authentication traffic, session setup, and key exchange against both classical and future quantum threats. Hybrid design is valuable because no single cryptographic family should be assumed permanent in the face of rapid technological change [35]. By combining classical algorithms with post-quantum primitives, the framework can maintain interoperability while improving long-term security. The encryption layer should support confidentiality, integrity, authentication, and key freshness. In principle, the hybrid construction can be represented by dual protection

$$K = H(K_{classical}, K_{pq}) \quad (7)$$

where the final key depends on both traditional and post-quantum inputs. This means the compromise of one component does not automatically collapse the whole system [36]. The design should also account for performance overhead, since cloud authentication requires responsiveness. Therefore, the cryptographic workflow must be secure but efficient.

5.1. Cryptographic Design Principles

The design principles of the cryptographic layer should include defence in depth, algorithm agility, forward secrecy, and composability. Defence in depth means the system does not rely on one primitive or one trust assumption [37]. Algorithm agility allows cryptographic components to be replaced as standards evolve or vulnerabilities emerge. Forward secrecy ensures that compromise of long-term keys does not reveal past sessions. Composability is important because the hybrid system must work correctly when the outputs of multiple mechanisms are combined. A general security target can be written as $\Pr[\text{break}] \leq \epsilon$, where $\epsilon$is a small acceptable bound. The cryptographic design should ensure that the effective security of the combined scheme is not weaker than its strongest well-constructed part [38]. This is especially important for cloud authentication because the system must remain trustworthy under routine use, high load, and changing threat conditions.

5.2. Symmetric Encryption Component

The symmetric encryption component is responsible for protecting the actual data payload once a secure session key has been established. Symmetric cryptography is preferred for data encryption because it is fast, efficient, and suitable for high-volume cloud communication [39]. Modern authenticated encryption modes are typically used because they provide confidentiality and integrity at the same time. In the hybrid framework, the symmetric key $K_s$is derived after the key exchange phase and is used to encrypt session messages, tokens, and sensitive identity data. A basic representation of authenticated encryption is

$$C = Enc_{K_s}(M) \quad \text{and} \quad M = Dec_{K_s}(C) \quad (8)$$

where $M$is plaintext and $C$is ciphertext. If integrity is included, the system may also compute an authentication tag

$$T = MAC_{K_s}(M) \quad (9)$$

The symmetric layer must use strong key rotation and should never reuse keys across unrelated sessions. This provides efficiency without sacrificing security.

5.3. Post-quantum key exchange component

The post-quantum key exchange component provides a secure way to establish shared secrets even in the presence of a quantum adversary. Its purpose is to replace or supplement classical key exchange methods that may become vulnerable over time [40]. In a hybrid design, the post-quantum secret is combined with a classical secret to derive the final session key, reducing dependence on any one primitive. Conceptually, the shared key can be expressed as

$$K = KDF(K_{cl} \parallel K_{pq}) \quad (10)$$

where $KDF$is a key derivation function and $\parallel$denotes concatenation. This composition helps ensure that even if one exchange method is later weakened, the other still contributes security [41]. The component should also support parameter negotiation, validation of public values, and resistance to tampering. For cloud authentication, this mechanism is critical because key exchange happens at the beginning of trust establishment and therefore protects all downstream communication.

5.4. Key management strategy

Key management is one of the most sensitive parts of the entire framework because even strong encryption can fail if keys are poorly handled. The strategy should define how keys are generated, stored, rotated, revoked, and destroyed [42]. Long-term keys should be protected using secure hardware modules or equivalent trusted storage, while short-term session keys should be ephemeral. The system should separate identity keys, session keys, and recovery keys so that compromise of one does not affect all others. A useful expression for key lifecycle risk is

$$R_k = P_e + P_s + P_r \quad (11)$$

where $P_e$is exposure risk during generation, $P_s$during storage, and $P_r$during reuse or revocation. Minimizing $R_k$requires strict access control, secure logging, and limited key visibility [43]. In cloud environments, distributed key management must also support synchronization across services without exposing raw secrets.

5.5. Encryption and decryption workflow

The encryption and decryption workflow describes how data moves securely through the hybrid system. During encryption, the client or gateway initiates a hybrid key exchange, derives a session key, and then encrypts the payload using symmetric authenticated encryption [44]. During decryption, the receiving side verifies the authenticity of the key exchange, reconstructs the same session key, and decrypts the message only if integrity checks pass. A simplified workflow may be written as

$$K_s = KDF(K_{cl} \parallel K_{pq}) \quad (12)$$

followed by $C = Enc_{K_s}(M)$and $M = Dec_{K_s}(C)$. This structure keeps the actual payload encryption fast while making key establishment resilient. The workflow should also support rekeying, so that long sessions do not depend on one static secret. In practice, this is essential for cloud systems where messages, tokens, and authentication artifacts may be exchanged repeatedly during a user session.

6. Behavioural Biometrics Module

The behavioural biometrics module adds a dynamic identity layer that observes how the user interacts with the system over time. Unlike passwords or OTPs, behavioural traits are difficult to transfer or steal in a simple way, making them attractive for continuous authentication [45]. The module must be able to capture user interaction signals, extract meaningful features, and compare them against an enrolled profile. Since behaviour changes naturally due to fatigue, environment, and device differences, the module should tolerate some variation while still detecting suspicious deviations. A generic scoring model can be written as $B = h(F_1, F_2, \dots, F_n)$, where $F_i$are behavioral features and $B$is the confidence score. The purpose of this module is not to replace

cryptographic authentication but to complement it by reducing the chance of unauthorized session continuation. In cloud settings, this is especially valuable because users often remain active for long periods after login.

6.1. Biometrics modality selection

Modality selection is the process of deciding which behavioural signals are most suitable for the target environment. Common choices include keystroke dynamics, mouse movement, touch gestures, scroll patterns, and device interaction timing. The selection should depend on usability, device diversity, threat exposure, and data quality. For example, a desktop-oriented system may rely more on keyboard and mouse features, while a mobile system may prefer touch and motion patterns [46]. The goal is to choose signals that are stable enough for authentication but still hard for an attacker to imitate accurately. A practical selection criterion can be described as

$$Q = \lambda R - \mu N + \nu U \tag{13}$$

where $R$is recognition power, $N$is noise sensitivity, and $U$is usability. The best modality is not always the richest one; it is the one that balances discriminability and deployment feasibility. This choice strongly influences later stages such as feature extraction and matching.

6.2. Feature extraction

Feature extraction transforms raw behavioural signals into measurable attributes that can be used for authentication. For keystroke dynamics, features may include dwell time, flight time, typing rhythm, and key press intervals [47]. For mouse or touch behaviour, features may include trajectory curvature, speed, pressure, dwell points, and movement variance. Good features should be stable for the same user but different enough across users to support discrimination. The extracted feature vector may be represented as

$$\mathrm{x} = [x_1, x_2, \dots, x_m] \tag{14}$$

Authentication then uses a similarity or classification function $s = f(\mathrm{x}, \mathrm{p})$, where pis the stored profile. High-quality features reduce false matches and improve robustness against spoofing. However, feature extraction must also be computationally efficient, because continuous authentication may run frequently in the background [48]. This makes feature design a central part of system performance and accuracy.

6.3. Template generation and storage

Template generation is the process of creating a reference representation of a user's behavioural profile during enrolment. The template may be a statistical model, centroid, classifier parameters, or protected feature representation rather than raw biometric data. Storage must be handled carefully because biometric templates are sensitive and potentially difficult to replace if exposed [49]. Therefore, the framework should use protected storage and avoid keeping unnecessary raw data. A template can be represented as

$$\mathrm{p} = T(\mathrm{x}_1, \mathrm{x}_2, \dots, \mathrm{x}_n) \tag{15}$$

where $T$is the model-building function. The storage design should also allow template updates to reflect natural behavior drift while preventing unauthorized modification. If templates are changed too slowly, the system may reject legitimate users; if changed too quickly, it may absorb attacker behaviour [50]. This balance is a critical design issue in behavioral authentication.

6.4. Continuous authentication

Continuous authentication monitors behaviour throughout the session rather than only at the login stage. This is particularly useful in cloud systems because attackers may take over a session after the initial authentication is complete. Continuous authentication evaluates live user interaction and compares it with the expected profile at regular intervals or event triggers. The process can be modelled as repeated scoring $B_t = h(\mathbf{x}_t)$over time t, with access maintained only if $B_t \geq \theta$. If the score falls below the threshold for too long, the system may require re-authentication or terminate the session [51]. The value of continuous authentication lies in its ability to detect gradual misuse, stealthy intrusions, and account sharing. It is best implemented in a way that is mostly invisible to the user, so that security improves

without adding constant interruptions. This makes it especially suitable for enterprise cloud access.

6.5. Spoofing resistance and liveness detection

Spoofing resistance ensures that the behavioural biometric module can distinguish real user behaviour from imitation, replay, or synthetic input. Liveness detection helps confirm that the observed activity is generated by a live human user rather than an automated script or captured trace [52]. The framework should combine temporal features, context awareness, anomaly detection, and challenge-response logic where appropriate. An attacker may try to replay recorded mouse traces or mimic typing patterns, so the system must look beyond static signature matching. One way to describe spoof resistance is by minimizing the attack success rate ASR, where

$$ASR = \frac{\text{successful spoofs}}{\text{spoof attempts}} \tag{16}$$

The system should also monitor for unnatural regularity, impossible timing patterns, or device-level inconsistencies. Effective spoofing resistance is essential because behavioural biometrics is only valuable if it can detect imitation and replay reliably.

7. Authentication Protocol Design

The authentication protocol design defines how users are enrolled, validated, monitored, and removed from the system. A protocol is needed because the framework must coordinate cryptographic exchange, biometric evaluation, session issuance, and revocation in a structured way [53]. The protocol should be secure, efficient, and suitable for integration with cloud identity services. It also needs to support adaptive decisions so that authentication strength can increase when risk is elevated. A general protocol outcome may be modelled as $A_t = f(K_t, B_t, R_t)$, where $A_t$is the authentication decision at time t, $K_t$is cryptographic validity, $B_t$is biometric confidence, and $R_t$is contextual risk. The protocol should treat enrollment as a trusted setup stage and make later stages more flexible but still secure. This section therefore describes the lifecycle of authentication from first registration to re-authentication and revocation.

7.1. Enrolment phase

The enrolment phase establishes the initial trust relationship between the user and the system. During enrolment, the user's behavioural profile is captured over multiple sessions to build a stable baseline. At the same time, the system may register cryptographic credentials, device identifiers, and policy attributes [54]. Because enrolment is the foundation of all later verification, it must be carefully protected against impostors. The protocol may require the user to prove identity through a stronger initial process before the biometric template is accepted. The enrolment result can be represented as $\mathrm{P}_0 = g(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_n)$, where $\mathrm{P}_0$is the stored profile. A secure enrollment phase should also define how templates are protected, how long raw observations are retained, and how later updates are approved. If enrollment is weak, the entire system's security is weakened from the start.

7.2. Initial login phase

The initial login phase is the first operational authentication check performed when a user attempts access. In this phase, the system verifies the user's cryptographic material, such as a password-derived factor, device token, or post-quantum key exchange result, and then evaluates the behavioural signal collected during the login interaction. This dual-step approach prevents reliance on one factor alone [55]. If both checks succeed, the system can issue a session token or secure context for cloud access. A simplified login decision may be written as

$$D_0 = \mathbb{1}(C_0 \wedge B_0) \tag{17}$$

where $C_0$is cryptographic success and $B_0$is biometric success. The login phase should be fast enough to avoid user frustration but strong enough to stop impersonation attempts. It also sets the confidence baseline for the rest of the session. This makes it a critical transition from identity proof to ongoing access.

7.3. Multi-factor verification phase

The multi-factor verification phase adds additional assurance by combining multiple independent proofs before granting or continuing access. These factors may include something the user knows, something the user has, something the user is, and contextual properties such as device posture or location [56]. In the proposed framework, behavioural biometrics acts as a continuous layer rather than a one-time input, while the cryptographic layer protects the communication and key exchange. The combined factor score can be expressed as

$$S = \sum_{i=1}^{n} w_i \, s_i \tag{18}$$

where $s_i$are factor scores and $w_i$are weights with $\sum w_i = 1$. If the score exceeds the threshold, access is allowed; otherwise, the system may step up verification. This phase is useful because no single factor is perfect, and combining them improves resilience against password theft, device compromise, or replay. The verification phase therefore acts as a risk-balanced control point.

7.4. Session establishment

Session establishment occurs after the user has passed the required verification checks and the system has decided to grant access. During this phase, secure session keys are created, tokens are issued, and policy constraints are attached to the session [57]. The session should be bound to the authenticated user, device, and risk context to prevent token reuse in a different environment. A typical representation of secure session creation is

$$Sess = Enc_{K_s}(ID, time, policy) \tag{19}$$

where the session context is protected by the established key. The session should also include expiry time, renewal rules, and revocation hooks. Strong session establishment is important because most post-login attacks target active sessions rather than the login page itself. By binding the session to both cryptographic and behavioral evidence, the framework reduces the chance of unauthorized continuation. This is especially important in cloud environments where sessions may span multiple services and long durations.

7.5. Re-authentication and revocation

Re-authentication and revocation are the mechanisms that keep a session trustworthy after it has started. Re-authentication may be triggered by time, risk changes, device movement, unusual behaviour, or service sensitivity [58]. Revocation occurs when the system determines that the session or credential can no longer be trusted. This may happen after repeated biometric failures, suspicious context, lost device reports, or policy violations. A practical re-authentication trigger can be modelled as $R_t = \mathbb{1}(B_t < \theta_1 \vee C_t < \theta_2 \vee X_t > \theta_3)$, where biometric confidence, cryptographic health, and contextual risk jointly determine whether action is needed. Revocation should be fast and comprehensive so that compromised tokens cannot continue to operate. A good design also ensures that revoked sessions cannot be silently restored without fresh verification. This final stage closes the loop between authentication and ongoing trust management.

8. Implementation Strategy

This section describes how the proposed framework can be built and deployed in a real cloud environment. The implementation should combine secure client software, cloud-side authentication services, cryptographic libraries, and biometric processing components into one coordinated system [59]. A practical architecture needs to support compatibility with existing IAM and KMS services while also allowing future algorithm updates as post-quantum standards evolve. Logging, telemetry, and audit support are also essential because cloud authentication must be observable and traceable during operations. The implementation goal is not only to make the design work technically, but also to make it maintainable, measurable, and secure in production.

8.1. Software and hardware setup

The software and hardware setup should include a client application, a secure cloud authentication service, a biometric feature extraction module, a post-quantum cryptographic library, and a centralized policy engine. On the client side, the system may run on desktops, laptops, or mobile devices with access

to keyboard, mouse, touch, or motion input depending on the biometric modality [60]. On the server side, the system should be deployed on cloud instances or containerized microservices with secure storage for keys, templates, and logs. Hardware acceleration such as TPM, HSM, or secure enclave support can improve protection for secrets and reduce exposure during cryptographic operations. The setup should also support testing on realistic network conditions so that latency, throughput, and failure handling can be evaluated accurately.

8.2. Client module implementation

The client module is responsible for collecting behavioural signals, managing local authentication artifacts, and securely communicating with the cloud service. It should capture data such as typing rhythm, mouse trajectory, or touch patterns, then transform them into feature vectors for verification [61]. The module should also handle secure key exchange initiation and transmit only the minimum required behavioural data to the backend to preserve privacy. A lightweight local decision step can be used to block obviously suspicious activity before it reaches the server, reducing unnecessary overhead. For example, if the local biometric confidence score is $B_c$and the threshold is θ, then access can be locally flagged when $B_c < \theta$. This improves responsiveness and supports the principle of edge-assisted security.

8.3. Cloud service implementation

The cloud service should host the authentication engine, risk analyser, policy manager, and session controller. Its main role is to validate cryptographic material, compare behavioural evidence, and issue access decisions for cloud resources. The service can be implemented as a set of microservices, allowing separate scaling of biometric analysis, key management, and token handling [62]. This modular structure makes it easier to monitor performance and update algorithms without interrupting the entire system. The service should also support anomaly detection for continuous authentication, since behavioural biometrics is strongest when combined with ongoing monitoring. In practice, the backend should expose secure APIs for enrolment, login, re-authentication, revocation, and audit retrieval.

8.4. Integration with IAM and KMS

Integration with IAM and KMS is necessary so the proposed framework can fit into enterprise cloud security rather than operate as a standalone prototype. The IAM system should manage identities, roles, policies, and access scopes, while the KMS should handle secure key creation, rotation, storage, and destruction. The biometric and cryptographic decisions from the framework should feed into IAM policy enforcement, so that access can be granted conditionally based on both user identity and session confidence [63]. A useful rule is $A = I \cap K \cap B$, where $I$is IAM authorization, $K$is key validity, and $B$is biometric confidence. This ensures that access is not granted unless all required controls agree. Integration also improves operational consistency because administrators can use existing governance workflows, logging tools, and incident response processes.

8.5. Logging and monitoring

Logging and monitoring are essential for security, auditing, and system improvement. The framework should record authentication attempts, confidence scores, key events, session changes, policy decisions, and revocation actions in a tamper-resistant manner. Logs should be structured so that suspicious patterns can be detected, such as repeated failed biometrics, unusual session renewals, or repeated key negotiation errors [64]. Monitoring dashboards can track metrics like authentication success rate, false rejection rate, latency, and anomalous access patterns. In continuous authentication, log-based visibility helps security teams understand why a session was flagged or terminated. The system can also compute a simple alert score

$$S_a = w_1F + w_2R + w_3L \tag{20}$$

where $F$is failure count, $R$is risk, and $L$is log anomaly level. Proper logging supports both forensic analysis and compliance obligations.

9. Security Analysis

Security analysis evaluates how well the proposed framework protects against confidentiality loss, unauthorized modification, quantum attacks, biometric spoofing, and network-level attacks. Because the system uses both cryptographic and biometric controls, the analysis must consider multiple attack surfaces at once. A layered system is stronger when each layer compensates for the weakness of another. The main security question is whether an attacker can bypass the system without possessing valid credentials, valid behaviour, and valid session context simultaneously. A simple expression for overall compromise probability is $P_{comp} = P_k \cdot P_b \cdot P_s$, where $P_k$is cryptographic compromise, $P_b$is biometric compromise, and $P_s$is session compromise. Lowering each term is the goal of the design. The following subsections analyze the major security properties in more detail.

9.1. Confidentiality analysis

Confidentiality means that sensitive authentication data, templates, keys, and session payloads remain unreadable to unauthorized parties. The framework protects confidentiality through hybrid encryption, secure key exchange, and controlled access to biometric data. Behavioural data should be transmitted and stored in protected form so that even if logs or traffic are intercepted, the attacker cannot reconstruct the user's profile. If the encryption layer uses authenticated encryption, then both secrecy and tamper detection are provided. The confidentiality level may be summarized by

$$C = 1 - P_{leak} \tag{21}$$

where $P_{leak}$is the probability of data exposure. Strong confidentiality also depends on key management, because a secure cipher cannot compensate for exposed keys. This makes cryptographic hygiene and access control central to the security model.

9.2. Integrity analysis

Integrity ensures that biometric templates, authentication messages, session tokens, and policy decisions cannot be altered without detection. The system should use authenticated encryption, message authentication codes, and secure transport to protect integrity across all communication channels. In the cloud setting, integrity is especially important because tampered authentication requests or modified session tokens can lead to privilege escalation. The integrity condition can be expressed as $I = 1 - P_{tamper}$, where $P_{tamper}$is the probability that an adversary can modify data successfully. The framework should verify message freshness and sequence consistency to prevent replay or substitution attacks. Integrity logging also helps detect unauthorized changes in stored templates or policy settings. This makes the architecture more trustworthy during both enrolment and operational use.

9.3. Resistance to quantum attacks

Resistance to quantum attacks is one of the main reasons for using a hybrid design. Classical public-key cryptography may eventually be weakened by quantum algorithms, so the framework includes post-quantum key exchange and related protections. If the final session key is derived from both classical and post-quantum inputs, then compromising the classical side alone does not reveal the full key. This can be represented as

$$K = KDF(K_{cl} \parallel K_{pq}) \tag{22}$$

which provides redundancy in key establishment. The design should also allow algorithm agility so that newer quantum-safe schemes can replace older ones as standards mature. This approach reduces migration risk and supports long-term security planning. Quantum resistance is therefore built into the system architecture rather than added later as a patch.

9.4. Resistance to biometric attacks

Resistance to biometric attacks means the system can handle spoofing, impersonation, replayed behaviour, and adversarial manipulated inputs. Behavioural biometrics is useful because imitation is difficult, but it is not immune to attack. The framework should use liveness detection, temporal analysis, anomaly detection, and confidence thresholds to reduce false acceptance. If an attacker replays recorded mouse paths or automated typing patterns, the system should detect unnatural regularity or

mismatch with current context. The attack success rate can be written as

$$ASR = \frac{N_{success}}{N_{attempt}} \quad (23)$$

and the objective is to keep ASRas low as possible. The system should also account for natural behavior drift so that legitimate users are not incorrectly rejected. This balance between robustness and tolerance is central to reliable biometric authentication.

9.5. Side-channel and replay attack analysis

Side-channel attacks exploit information such as timing, power use, or observable behaviour during computation, while replay attacks reuse previously captured messages or biometric traces. To resist side-channel exposure, the implementation should minimize information leakage from cryptographic operations and protect secret handling with secure hardware where possible. Randomization, constant-time execution, and secure enclaves can further reduce leakage risk. Replay resistance requires nonces, timestamps, challenge-response validation, and session freshness checks. A simple replay validity rule is

$$V = \mathbb{1}(t_{recv} - t_{send} < \Delta) \quad (24)$$

where $\Delta$is the acceptable freshness window. If a message falls outside the window or repeats an earlier nonce, it must be rejected. These protections are important because many authentication failures arise not from breaking encryption, but from reusing old valid data in a new context.

10. Performance and Evaluation

Performance evaluation measures whether the proposed framework is practical, efficient, and accurate enough for cloud deployment. A secure system that is too slow or too resource-intensive may not be suitable for real users. Therefore, evaluation should examine authentication accuracy, latency, throughput, scalability, and operational overhead. The framework should be tested under realistic workload conditions and with realistic behavioural variation. A general performance objective is to maximize security benefit while minimizing cost, which can be expressed as $\max \frac{S}{O}$, where $S$is security gain and $O$is operational overhead. Continuous authentication systems also need evaluation over time because behavior changes and long sessions can reveal drift effects. The following subsections outline the core evaluation dimensions.

10.1. Evaluation metrics

The evaluation metrics should include authentication accuracy, false acceptance rate, false rejection rate, equal error rate, latency, throughput, CPU usage, memory usage, and key establishment overhead. For biometric systems, the most common metrics are TAR, FAR, FRR, and EER, which show how well the system distinguishes legitimate users from impostors. Cryptographic evaluation should include handshake latency and session setup cost, especially because hybrid encryption may add computation. A general accuracy measure is

$$Acc = \frac{TP+TN}{TP+TN+FP+FN} \quad (25)$$

where TP, TN, FP, and $FN$are the usual classification outcomes. These metrics together provide a balanced view of both security and usability. The framework should be evaluated not only on one-time login accuracy but also on continuous-session reliability.

10.2. Experimental setup

The experimental setup should define the hardware, software, datasets, and testing conditions used to evaluate the framework. It should include client devices, cloud instances, network conditions, and the behavioural data collection environment. The testing process should simulate realistic user sessions with both legitimate and malicious activity. If possible, different device types and input modalities should be included to test generalization. The setup should also document the cryptographic algorithms used, the biometric feature set, and the policy thresholds. Reproducibility is important, so parameter values and measurement procedures should be recorded carefully. This allows others to understand how the reported results were obtained and whether the framework is likely to work under similar

conditions. A well-defined setup improves the credibility of the entire evaluation.

10.3. Authentication accuracy

Authentication accuracy measures how well the framework accepts legitimate users and rejects impostors. In this design, accuracy depends on both the cryptographic result and the biometric confidence score. A useful representation is $A = w_1 A_c + w_2 A_b$, where $A_c$is cryptographic accuracy and $A_b$is biometric accuracy. The framework should aim for a low false acceptance rate because unauthorized access is more damaging than occasional inconvenience to users. At the same time, false rejection must also be controlled so that legitimate users are not frequently blocked. Continuous authentication tends to improve security but can increase false alarms if thresholds are too strict. Therefore, accuracy should be measured across different thresholds and user conditions to identify the best operating point. This makes the system more robust and practical for deployment.

10.4. Latency and throughput

Latency and throughput determine how quickly the system can authenticate users and how many requests it can process under load. Latency includes the time for cryptographic negotiation, biometric feature processing, policy evaluation, and session issuance. Throughput measures how many authentication events the system can handle per second or minute. Because the framework uses hybrid encryption and continuous biometric checks, the performance overhead must be carefully controlled. The total delay can be modelled as

$$T_{total} = T_{crypto} + T_{bio} + T_{policy} + T_{net} \qquad (26)$$

The design should keep T_{total}low enough that users do not perceive the system as slow. Throughput testing should also include concurrent users to simulate real cloud demand. This is important because cloud systems must remain responsive even during peak access periods.

10.5. Scalability and overhead analysis

Scalability analysis examines how the system behaves as the number of users, sessions, and authentication checks increases. A scalable design should maintain acceptable performance even when deployed across large cloud environments. Overhead includes CPU cost, memory use, network traffic, storage usage, and administrative burden. Since behavioural biometrics requires ongoing monitoring, the system must be careful not to create excessive resource demand. Overhead may be summarized as

$$O = O_c + O_b + O_l \qquad (27)$$

where $O_c$is cryptographic overhead, $O_b$biometric overhead, and $O_l$logging overhead. The framework should be evaluated at multiple scales to determine whether bottlenecks appear in client processing, backend analysis, or key management. A practical system must remain efficient as it grows, not only in small test cases but also under realistic enterprise loads.

11. Privacy and Compliance

Privacy and compliance are essential because the framework processes sensitive identity data and behavioural biometric information. Unlike ordinary credentials, biometric traits are personal, persistent, and potentially difficult to replace if compromised. The system should therefore follow strong privacy-by-design principles and align with relevant legal and ethical expectations. Compliance is not only about avoiding penalties; it also increases user trust and supports responsible deployment. A general privacy objective is to minimize unnecessary data exposure while preserving authentication utility, which can be expressed as $\min P_{expose}$subject to $U \geq U_{min}$. The framework should also support auditability so that policy decisions can be reviewed later if needed. These requirements shape how data is collected, stored, processed, and deleted.

11.1. Data minimization

Data minimization means collecting only the information needed for authentication and no more. In the proposed framework, this principle is especially important for behavioural biometrics because raw interaction traces can reveal more than just identity. The system should therefore rely on derived features or

protected templates instead of raw streams whenever possible. It should also limit retention periods and reduce the number of services that can access biometric data. A minimal data policy can be described by $D_{store} = \arg\min D$ subject to authentication performance remaining acceptable. The less unnecessary data that is retained, the lower the privacy exposure. This principle also reduces the impact of a breach because there is less sensitive material available to steal.

11.2. Template protection

Template protection is necessary because biometric templates are not like passwords and cannot easily be replaced if leaked. The framework should protect templates through hashing, transformation, secure storage, or cancellable biometric methods. It may also use encrypted storage, secure enclaves, or protected KMS-backed repositories for template handling. A protected template may be represented as

$$T_p = H(T \parallel s) \tag{28}$$

where $H$is a cryptographic transformation and $s$is a secret salt or transform key. The purpose is to prevent reconstruction of the original behavioral signal from stored data. Template protection should also support updates and revocation without exposing the raw biometric history. This is one of the most important privacy safeguards in the whole design.

11.3. Consent and user privacy

Consent and user privacy require that users understand what data is being collected, why it is collected, and how it will be used. Because behavioural biometrics can feel less visible than passwords or OTPs, transparency is especially important. The system should present clear notices about enrolment, continuous monitoring, storage periods, and revocation policies. Users should also be given meaningful control over participation where the application context allows it. A consent-aware design increases trust and aligns the framework with ethical deployment. Privacy can also be reinforced by providing explanations when the system requests re-authentication or denies access. This helps users understand that the system is responding to risk rather than acting arbitrarily.

11.4. Regulatory considerations

Regulatory considerations include data protection laws, sector-specific rules, and organizational governance requirements. Depending on deployment context, the framework may need to align with GDPR, CCPA, or other privacy frameworks, especially when biometric data is processed across jurisdictions. Regulatory design should consider lawful basis, purpose limitation, storage limitation, access rights, and breach response. Since cloud systems often operate internationally, the framework should be able to support region-specific storage and processing policies. Compliance is easier when the system has clear logging, documented retention rules, and access restrictions. A compliance score can be thought of as $G = f(P, A, R)$, where $P$is policy alignment, $A$is audit quality, and $R$is regulatory readiness. This section is important because technical security alone does not guarantee lawful or responsible deployment.

11.5. Audit and accountability

Audit and accountability ensure that decisions made by the framework can be traced, reviewed, and justified. Every major action such as login, re-authentication, session revocation, key rotation, and template update should leave a secure record. These records help with incident response, compliance review, and system debugging. Accountability also means the system should be able to explain why access was granted or denied, at least in policy terms. A simple audit function may be written as

$$A_u = \{e_1, e_2, \ldots, e_n\} \tag{29}$$

where each $e_i$is a security event. Proper audit trails improve trust because they make hidden failures easier to detect. They also support governance by showing that the system is operating according to approved rules.

12. Limitations and Future Work

No authentication framework is perfect, and this proposal has limitations that should be acknowledged clearly. Behavioural biometrics can be affected by noise, user fatigue, device

differences, and gradual drift over time. Hybrid encryption adds complexity because multiple cryptographic mechanisms must be managed correctly. Cloud deployment also introduces practical constraints such as integration difficulty, operational overhead, and policy coordination across services. These limitations do not invalidate the design; they show where additional engineering and research are needed. A realistic future path should improve robustness, reduce overhead, and make the system easier to adopt. The following subsections outline the main gaps and future directions.

12.1. Current limitations

The current limitations include dependence on high-quality behavioural data, potential false rejections, template sensitivity, and the cost of implementing and maintaining hybrid cryptography. Continuous authentication can be effective, but it may not work equally well across all users or devices. Different environments may produce different input patterns, which can reduce consistency. The system also relies on correct threshold tuning, and poor parameter choices can weaken both security and usability. Another limitation is that the framework assumes the biometric modality is available and stable enough to support recognition. In practical deployments, this may not always be true. These limitations suggest that the model should be deployed gradually and tested carefully before large-scale adoption.

12.2. Deployment challenges

Deployment challenges include integrating the framework with existing cloud infrastructure, ensuring compatibility with IAM and KMS, and coordinating policies across multiple services. Another challenge is balancing security with performance, since cloud systems must remain responsive under load. Behavioural biometrics may also face organizational resistance because it introduces new privacy and governance concerns. Security teams may need additional training to manage post-quantum algorithms and biometric workflows. There is also the challenge of secure client-side implementation across diverse devices and operating systems. These issues mean the framework cannot be treated as a drop-in replacement; it requires careful planning, testing, and staged rollout.

12.3. Future enhancements

Future enhancements may include federated learning for biometric model updates, stronger privacy-preserving template protection, improved risk scoring, and more efficient post-quantum primitives. The system could also incorporate device attestation, contextual AI, and adaptive trust policies to improve decision quality. Another useful direction is to improve explainability so that authentication decisions are easier to interpret by users and administrators. Future versions might also support multi-modal behavioural input, combining several signals for better accuracy. If standardized post-quantum algorithms become more efficient, the framework can update its cryptographic layer without redesigning the entire system. This kind of algorithm agility is one of the strongest long-term benefits of the proposed approach.

12.4. Research directions

Future research should investigate how behavioural drift affects long-term authentication accuracy and how to retrain models safely without exposing sensitive data. Another direction is to examine how quantum-safe authentication can be deployed at large scale across hybrid and multi-cloud architectures. It would also be valuable to study explainable security policies that clarify why the system changes its authentication strength over time. Research could further explore secure, privacy-preserving ways to compare behavioural templates without revealing raw features. Side-channel hardening and replay resistance in real hardware deployments are also important areas for continued work. These directions can help move the framework from a conceptual model to a mature operational solution.

13. Conclusion

The proposed framework brings together quantum-resilient hybrid encryption and behavioural biometrics to strengthen multi-layer cloud authentication. It addresses current threats such as credential theft and session hijacking while also preparing for future

quantum risks. By combining cryptographic protection with continuous behavioural verification, the framework creates a more adaptive and resilient security model. The design also emphasizes privacy, compliance, logging, and operational feasibility so that it can be considered for real-world cloud deployment. Overall, the approach demonstrates that strong authentication should be both forward-looking and practical. The final value of the framework lies in its layered defence, where each component reinforces the others.

References:

[1] Shrivastava, A., Hundekari, S., Praveen, R. V. S., MuhsnHasan, M., Lakhanpal, S., & Bansal, S. (2025, September). Edge-Slicing for URLLC and mMTC in Integrated Satellite-Terrestrial 5G Networks. In 2025 International Conference on Computing and Communications (COMPUTINGCON) (pp. 1-7). IEEE.

[2] Nutalapati, P., Dhavale, S. M., Shrivastava, A., Praveen, R. V. S., Vemuri, H. K., & RiadHwsein, R. (2025, August). IoT and Machine Learning-Enhanced Energy Management in Enabled Smart Grids for Predictive Load Balancing. In 2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS) (pp. 1-6). IEEE.

[3] Thayumanavan, K., Kumar, A., Praveen, R. V. S., Bhendale, M. A., & Agnihotri, K. (2025, August). Hybrid Transformer Based Framework for Enhanced Financial Market Analysis and Online Trading Forecasting. In 2025 2nd International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-6). IEEE.

[4] Patil, B. D., Praveen, R. V. S., Rambhatla, A. K., Trakroo, K., Singh, K., & Vishanth, R. (2025, August). Graph Neural Network Model for Intelligent Urban Traffic Flow Prediction and Smart City Mobility Management. In 2025 2nd International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-6). IEEE.

[5] Chandra, N. S., Rao, K. S., Praveen, R. V. S., Upadhye, N. A., & Kaliappan, S. (2025, August). Hybrid Auto-Encoder Framework for Water Pollution Prediction in Smart Cities. In 2025 2nd International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-6). IEEE.

[6] Victor, S., Kumar, K. R., Praveen, R. V. S., Aida, R., Kaur, H., & Bhadauria, G. S. (2025, August). GAN and RNN Based Hybrid Model for Consumer Behavior Analysis in E-Commerce. In 2025 2nd International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-6). IEEE.

[7] Srinivas, A. C. M. V., Hemavathi, U., Devi, G. U., Praveen, R. V. S., Vasumathi, G. G., & Saranya, R. (2025, August). Secure and Intelligent Framework for Kidney Stone Detection Using a CNN-XGBoost Hybrid Model with Blockchain Integration. In 2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS) (pp. 1-6). IEEE.

[8] Kumar, S., Shrivastava, A., Praveen, R. V. S., Subashini, A. M., Vemuri, H. K., & Alsalami, Z. (2025, August). Future of Human-AI Interaction: Bridging the Gap with LLMs and AR Integration. In 2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS) (pp. 1-6). IEEE.

[9] Choudhari, P., Tatiya, M., Praveen, R. V. S., Kaur, H., Vemuri, H. K., & MuhsnHasan, M. (2025, August). Enhancing Energy Efficiency in IoT Networks Using Deep Learning-Based Predictive Maintenance. In 2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS) (pp. 1-6). IEEE.

[10] Shrivastava, A., Praveen, R. V. S., Aida, R., Vemuri, K., Vemuri, S. S., & Husain, S. O. (2025, August). A Comparative Analysis of Graph Neural Networks for Social Network Data Mining. In 2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS) (pp. 1-6). IEEE.

[11] Jadhav, S., Chakrapani, I. S., Sivasubramanian, S., RamKrishna, B. V., Mouleswararao, B., & Gangwar, S. (2025). Designing Next-Generation Platforms with Machine Learning to Optimize Immune Cell Engineering for Enhanced Applications. Trends in Immunotherapy, 226-244.

[12] Vijayakumar, L., Kannadasan, B., Hinge, P., Reddy, L. K. K., Praveen, R. V. S., & Kalidindi, N. (2025, September). Analysis and Prediction of Employee Turnover with Effective Feature Selection based on Lee–Carter and ANN Model. In 2025 2nd Asia Pacific Conference on Innovation in Technology (APCIT) (pp. 1-6). IEEE.

[13] Dhanabal, S., Goswami, C., Praveen, R. V. S., & Vetriselvi, T. (2025). Shuffle-F-ZFNet: ShuffleNet Fuzzy Zeiler and Fergus network for data aggregation in WSN data communication. Wireless Networks, 31(6), 4111-4134.

[14] Thamma, S. R., Gurumoorthi, E., Prakash, C. O., Muthusundar, S. K., Nidhya, M. S., & Maram, B.

(2025, March). Comparison of SVM and Random Forest for Detection of Malicious Node in Wireless Sensor Networks. In 2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS) (pp. 1637-1643). IEEE.

[15] Hundekari, S., Shrivastava, A., Mhsnhasan, M., Praveen, R. V. S., Labde, V. V., & Yadav, K. (2025). Link Prediction in Graph-Based Data: Techniques for Analyzing and Predicting Network Connections. In Graph Mining: Practical Uses and Instruments for Exploring Complex Networks (pp. 67-76). Cham: Springer Nature Switzerland.

[16] Maharajan, K., Parasar, A., Khurana, P., Praveen, R. V. S., Sathiyanathan, S., & Priti, C. (2025, July). Enhancing Business Education Through AI-Powered Teaching Innovations in Quantitative Subjects Using Neural Architecture Search with Self-Attention. In 2025 International Conference on Communication and Smart Devices (ICCoSD) (Vol. 1, pp. 1-6). IEEE.

[17] Mishra, P., Kalburgikar, A., Praveen, R. V. S., Soujanya, K., Balamurugan, S., & Kalra, G. (2025, July). A Graph Neural Network-Based Hybrid AI Model for Detecting Fake Reviews and Fraudulent Sellers to Enhance Trust in E-Commerce. In 2025 3rd World Conference on Communication & Computing (WCONF) (pp. 1-7). IEEE.

[18] Raja, M. W. (2019). A Novel Image Processing Algorithm Based On Pixel Approximation for Accurate Breast Cancer Identification and Segmentation.

[19] Kani, R. M., Kumar, K. S., Gasimov, J. Y., Praveen, R. V. S., Daniel, D. J. D., & Kumari, K. S. (2025, July). Stock Price Trend Prediction in the Banking Sector for Market Analysis and Investment Decision-Making Using a Hybrid Random Forest-LSTM Model. In 2025 3rd World Conference on Communication & Computing (WCONF) (pp. 1-6). IEEE.

[20] Tiwari, S. S., Kumar, S., Praveen, R. V. S., Kumar, G., Sekhar, S. C., & Bhokare, R. (2025, July). Automated Smart Attendance System for Higher Education using a Lightweight DNN Model-based Face Recognition. In 2025 8th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1513-1518). IEEE.

[21] Alfurhood, B. S., Danthuluri, M. S. M., Jadhav, S., Mouleswararao, B., Kumar, N. P. S., & Taj, M. (2025). Real-time heavy metal detection in water using machine learning-augmented CNT sensors via truncated factorization nuclear norm-based SVD. Microchemical Journal, 115375.

[22] Magdum, V. B., Adivarekar, P. P., Praveen, R. V. S., Kovalenko, A. B., & Kumar, B. S. (2025, May). Advanced Global Safety with Precision Disaster Prediction and Early Warning Systems Using HPReADS Models. In 2025 Global Conference in Emerging Technology (GINOTECH) (pp. 1-6). IEEE.

[23] Chauhan, P. R., Vanitha, P., Agnihotri, K., Praveen, R. V. S., Kumar, S., & Praveena, S. (2025, May). Analysing Social Entrepreneurship and Financial Inclusion for Women Empowerment Using an F-GNN and AXGB Hybrid Approach. In 2025 Global Conference in Emerging Technology (GINOTECH) (pp. 1-6). IEEE.

[24] Akhmetshin, E., Parasar, A., Praveen, R. V. S., & Gupta, S. (2025, May). Accurate Forecasting of Teacher Performance and Behaviour in Higher Education Using RNN-XGBoost Multilayer Model. In 2025 Global Conference in Emerging Technology (GINOTECH) (pp. 1-7). IEEE.

[25] NR, A. R., Rajasri, T., Praveen, R., Kalla, D., Bendale, S. P., & Venu, N. (2025, April). CAC Training-A Unified Cybersecurity Training Program for Military Staff. In 2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI) (Vol. 3, pp. 569-573). IEEE.

[26] Kalaiselvi, M., Dasa, S. K., Malik, N., & Praveen, R. V. S. (2025, July). Intrusion Detection and Security Challenges in 6G Networks Using Stochastic Graph Neural Networks. In 2025 International Conference on Information, Implementation, and Innovation in Technology (I2ITCON) (pp. 1-6). IEEE.

[27] Kumar, B. R., Ali, S. R. M., Praveen, R. V. S., Thangam, A., Malik, N., & Kalra, G. (2025, July). A Novel Optimized Hybrid LSTM-Based Dynamic Demand Forecasting Model for Resilient Supply Chains. In 2025 International Conference on Information, Implementation, and Innovation in Technology (I2ITCON) (pp. 1-6). IEEE.

[28] Uma, G. (2026). A Novel Trusted Key Support Model for Synchronized Data Protection in Duplicate-Aware Cloud Storage. Indian Journal of Science and Technology, 19(19), 1260-1266.

[29] Thamma, S. R., Devalampeta, B. R., & Jangareddy, M. R. (2025, January). Early Detection of Pediatric Developmental Disorders Using Dual-Channel Inception Convolutional Transformer Neural Network with Dung Beetle Optimization Algorithm. In 2025 International Conference on Next Generation Communication & Information Processing (INCIP) (pp. 961-966). IEEE.

[30] Rajput, N., Praveen, R. V. S., Shrivastava, A., Kulshreshtha, K., Shakir, A. M., Hadi, A. A. A. K., &

Majeed, D. A. (2025, July). Optimized K-Means Algorithm for Large-Scale Customer Segmentation in E-Commerce Platforms. In 2025 3rd International Conference on Cyber Resilience (ICCR) (pp. 1-7). IEEE.

[31] Jadhav, S., Aruna, C., Choudhary, V., Gamini, S., Kapila, D., & Reddy, C. P. (2025). Reprogramming the Tumor Ecosystem via Computational Intelligence-Guided Nanoplatforms for Targeted Oncological Interventions. Trends in Immunotherapy, 210-226.

[32] Manikandan, K., Moparthi, R., Praveen, R. V. S., Balasubramanian, K., KK, L., & Sivanantham, S. (2025, July). Lung Cancer Detection From CT Images Using Image Processing and Hybrid Neural Network Models. In 2025 International Conference on Information, Implementation, and Innovation in Technology (I2ITCON) (pp. 1-6). IEEE.

[33] Supraja, N. S., Praveen, R. V. S., Vemuri, H. K., Jaiswal, V. K., & Sista, S. (2025). Leveraging AI and ML in Central Bank Strategies for Financial Stability. Advances in Consumer Research, 2(4).

[34] Gudimella, A., Ram Gopal Peri, S. S. S., Praveen, R. V. S., Labde, V. V., Deshmukh, R., & Shrivastava, A. (2025). Green Finance and ESG Investing: Evaluating Impact on Corporate Valuation. Advances in Consumer Research, 2(3).

[35] Sujitha, B. B., Rao, C. V., Thiyagarajan, C., Shakhov, D., & Praveen, R. V. S. (2025, June). Intelligent Energy Consumption Estimation in IoT-Enabled Smart Homes Using a Hybrid CNN-GRU Model. In 2025 Second International Conference on Cognitive Robotics and Intelligent Systems (ICC-ROBINS) (pp. 140-145). IEEE.

[36] Kathiravan, M. N., Periyasamy, V. M., Kumar, P., Praveen, R., Chetana, S., & Surender, S. (2025, June). IoT-Integrated Graph Convolutional Networks and LSTM Models for Smart Plant Growth Monitoring in Controlled Environment Agriculture. In 2025 5th International Conference on Intelligent Technologies (CONIT) (pp. 1-5). IEEE.

[37] Jose, N., Daruvuri, R., Puli, B., Sundaramoorthy, P., & Praveen, R. V. S. (2025, June). An integrated context-aware adaptive meta-learning system for accurate risk estimation of postpartum depression. In 2025 11th International Conference on Communication and Signal Processing (ICCSP) (pp. 323-327). IEEE.

[38] Thamma, S. R., Devalampeta, B. R., Jangareddy, M. R., & Tanna, P. (2026). Confidential AI Prompt Sharing: A Block-chain Driven Framework for Secure Data Exchange. In Emerging Perspectives and Applications of Computational Intelligence and Smart Systems (pp. 363-368). CRC Press.

[39] Poonguzhali, C., Neethika, A., Yalagi, P. C. K., Praveen, R. V. S., Isaac, S., & Srivel, R. (2025, June). Transforming Mental Health Care through Clinical Decision Support System Surface Technology. In 2025 11th International Conference on Communication and Signal Processing (ICCSP) (pp. 474-479). IEEE.

[40] Bhuvaneswari, E., Prasad, K. D. V., Ashraf, M., Jadhav, S., Rao, T. R. K., & Rani, T. S. (2025). A human-centered hybrid AI framework for optimizing emergency triage in resource-constrained settings. Intelligence-Based Medicine, 12, 100311.

[41] Lavanya, K., Thangamani, M., Ganthimathi, M., Priyanka, S., Peter, V. J., & Sapthika, J. (2026). A Multi-Class Deep Neural Network Framework Driven Automated Classification Of Diabetic Retinopathy Using Retinal Fundus Images. Genetics and Molecular Research, 25(1).

[42] Khaire, S. A., Monica, C. L., Parasar, A., Praveen, R. V. S., Kalinskaya, E., & Dineshkumar, B. (2025, May). Enhancing Automated Assignment Assessment in Higher Education with a CNN–BiLSTM Model. In 2025 6th International Conference for Emerging Technology (INCET) (pp. 1-6). IEEE.

[43] Maniraj, S. P., Boddepalli, E., Avula, V. A., Praveen, R. V. S., Kaliappan, S., & Reddy, P. C. S. (2025, May). A Novel Framework for Automated Cervical Cancer Detection and Prediction using Graph Convolutional Neural Network-based Models. In 2025 3rd International Conference on Data Science and Information System (ICDSIS) (pp. 1-6). IEEE.

[44] Elumalai, J., Manoranjithem, V., Labde, V. V., Karpagavalli, S. M., & Praveen, R. V. S. (2025, May). Attention based Graph Convolutional Network for IoT Cybersecurity Anomaly Detection with Hyperparameter Sensitivity Analysis. In 2025 3rd International Conference on Data Science and Information System (ICDSIS) (pp. 1-6). IEEE.

[45] Mukherjee, S., Labde, V. V., Gopal Peri, S. S. S. R., Praveen, R. V. S., Gudimella, A., Deshmukh, R., & Shrivastava, A. (2025). Decentralized Finance (DeFi): A Paradigm Shift in Global Financial Systems. Advances in Consumer Research, 2(3).

[46] Jadhav, S., Durairaj, M., Reenadevi, R., Subbulakshmi, R., Gupta, V., & Ramesh, J. V. N. (2024). Spatiotemporal data fusion and deep learning for remote sensing-based sustainable urban planning. International Journal of System Assurance Engineering and Management, 1-9.

[47] Selvam, M., Srivani, M., Jose, N. N., Saravanabhava, P., Praveen, R. V. S., & Vijayalakshmi, P. (2025, April). Implementing a Resilient and Pairing-Free Aggregate Signature Scheme for Healthcare Internet of Things Networks. In 2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI) (Vol. 3, pp. 428-433). IEEE.

[48] Shahane, M. S., Rajasri, T., Praveen, R., SR, A. R., Bendale, S. P., & Venu, N. (2025, April). Optimizing the Placement of Virtual Network Functions for Energy Efficiency in a Wireless Mesh Network. In 2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI) (Vol. 3, pp. 580-585). IEEE.

[49] Nagarajan, S., Vijay, S., Karthi, S., Praveen, R. V. S., & Naresh, B. (2025, March). Enhancing IoT-Based Smart Farming Security with a Hybrid GRU Intrusion Detection System. In 2025 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI) (Vol. 3, pp. 1-6). IEEE.

[50] Sagili, S. R., Shibi, B., Praveen, R. V. S., & Anjana, P. (2025). Sentiment Classification for Depression Detection: Integrating Capsule Networks with CNNs on Review Data. 2025 Emerging Technologies for Intelligent Systems (ETIS), 1-7.

[51] Kukreti, S., Praveen, R. V. S., Bansal, S., Raju, H., Singh, N., & Begum, R. (2025, February). Object Detection in Real-Time Surveillance Using Deep Learning-Based YOLO Framework. In 2025 International Conference on Computational, Communication and Information Technology (ICCCIT) (pp. 601-606). IEEE.

[52] Malviya, M., Adhana, D. K., Praveen, R. V. S., Mishra, B. R., Madasu, P., & Haralayya, B. (2025). Adaptation to Integration A Review on the Indian Accounting Standards (Ind AS) in Global Financial Reporting Convergence.

[53] Raja, W., Chandraprabha, K., Ruckmani3b, V., & Gowri4c, S. (2026). Implementing LSTM-RNN for improved diabetic dataset classification.

[54] Thamma, S. R., Prajwala, N. B., Pushpa, N. B., & Patra, A. (2025). Neuroimaging: A Computational Lens on the Brain. In Visualization in Neuroanatomical Sciences (pp. 53-68). Cham: Springer Nature Switzerland.

[55] Chaubey, N. K., Dahiya, R., Venkateswaran, R., RVS, P., Hemavathi, U., & Subramaniam, S. (2025). Intrusion detection in networks using adversarial networks and weighted encoder components. In Advanced Cyber Security Techniques for Data, Blockchain, IoT, and Network Protection (pp. 413-434). IGI Global Scientific Publishing.

[56] Subburaj, T., Praveen, R. V. S., Devi, S. R., & Reddy, D. S. (2024, December). Enhancing Electricity Theft Detection and Loss Prediction in Metro Cites Using Hybrid Machine Learning Model. In 2024 Eighth International Conference on Parallel, Distributed and Grid Computing (PDGC) (pp. 865-870). IEEE.

[57] Shinkar, A. R., Joshi, D., Praveen, R. V. S., Rajesh, Y., & Singh, D. (2024, December). Intelligent solar energy harvesting and management in IoT nodes using deep self-organizing maps. In 2024 International Conference on Emerging Research in Computational Science (ICERCS) (pp. 1-6). IEEE.

[58] Mrudula, J., Praveen, R. V. S., Sowmya, V. J., Shinde, N. N., & Ganvir, P. S. (2024, December). Advanced IoT and machine learning solutions for sustainable groundwater management using edge-based residual graph attention network model. In 2024 International Conference on Emerging Research in Computational Science (ICERCS) (pp. 1-6). IEEE.

[59] Kemmannu, P. K., Praveen, R. V. S., & Banupriya, V. (2024, December). Enhancing Sustainable Agriculture Through Smart Architecture: An Adaptive Neuro-Fuzzy Inference System with XGBoost Model. In 2024 International Conference on Sustainable Communication Networks and Application (ICSCNA) (pp. 724-730). IEEE.

[60] Mohandas, R., Elavarasi, M., Praveen, R. V. S., Chittapragada, H., Nithiya, C., & Prabagar, S. (2024, December). Advanced cyber-attack detection in iot networks using deep belief networks and gradient boosting mechanisms. In 2024 4th International Conference on Mobile Networks and Wireless Communications (ICMNWC) (pp. 1-7). IEEE.

[61] Vandana, C. P., Basha, S. A., Madiajagan, M., Jadhav, S., Matheen, M. A., & Maguluri, L. P. (2024). IoT resource discovery based on multi faected attribute enriched CoAP: smart office seating discovery. Wireless Personal Communications, 1-18.

[62] Wange, N. J., Praveen, R. V. S., Babavali, S. F., Rao, P., Gamini, P., & Ramasamy, D. (2024, December). Optimizing Thermal Comfort and Energy Efficiency in Smart Buildings using GANs and Reinforcement Learning Models. In 2024 4th International Conference on Mobile Networks and Wireless Communications (ICMNWC) (pp. 1-6). IEEE.

[63] Subha, B., Nagarajan, S., Thangam, A., Srinivas, V. S., Praveen, R. V. S., & Bakshi, K. D. (2024, December). Fuzzy Clustering and Autoencoder-Based Cybersecurity for EVs in a

Blockchain-Enabled Smart Cloud Environment. In 2024 4th International Conference on Mobile Networks and Wireless Communications (ICMNWC) (pp. 1-7). IEEE.

[64] Bhagat, S. K., Thamma, S. R., Devalampeta, B. R., Jangareddy, M. R., Kumar, R., & Pandey, S. D. (2025, May). Smart Parallel Algorithm for Optimized Load Balancing in Cloud Computing. In 2025 2nd International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE) (pp. 1-6). IEEE.

Cite this article as: Dr. J. Mohammed Ubada., (2026). Quantum-Resilient Hybrid Encryption Framework with Behavioural Biometrics for Enhanced Multi-Layer Cloud Authentication. International Journal of Emerging Knowledge Studies. 5(6), pp. 974–995.
https://doi.org/10.70333/ijeks-05-07-008