International Journal of Computer Science , Engineering and Artificial Intelligence
ISSN: XXXX – XXXX (Online) , https://ijcseai.com/
Regular Issue, Vol. 3, Issue. 3 (July – September) , 2026 , Pages: 9 - 17
Received: 17 September 2025 ; *Accepted:* 30 June 2026 ; *Published:* 17 July 2026
https://doi.org/10.63328/IJCSEAI-V3RI3P2
https://www.youtube.com/watch?v=Kyhw0Bzpvuk
https://archive.org/details/jsp-ijcseai-v3ri3p2
Original Paper : Applied Research – Experimental Research Paper

Hybrid Quantum-Resistant Behavioural Authentication Framework for Cloud Systems Using Post-Quantum Cryptography and Behavioral Biometrics

Lava Kumar Vandrangi

Department of Information Systems & Engineering Management,
Harrisburg University of Technology and Sciences, Pennsylvania , USA

* *Corresponding Author : Lava Kumar Vandrangi ; lavakumar.af691@gmail.com*

Abstract: When it comes to cloud applications, authentication systems are a captive audience of increasingly applicable attacks that steal credentials and vulnerable authentication methods, as well as vulnerable applications that will soon be disrupted by a new problem: quantum computing. Mathematical algorithms such as RSA and Elliptic Curve Cryptography (ECC) algorithms are vulnerable to Shor's algorithm and behavioral solutions do not sufficiently provide the provable security to a regulated cloud environment. The proposed framework, QBAC, is a Quantum-Resistant Behavioral Authentication Framework which combines post-quantum key encapsulation (CRYSTALS-Kyber) with multi-modal behavioral biometric verification and session monitoring in real-time. All these characteristics are combined within a framework that synergizes keystroke, mouse, timing and regularity and feeds a machine-learning based classification model designed to calculate a real-time Authentication Confidence Score (ACS). A Continuous Trust Score (CTS) is being kept in each cloud session that allows for anomaly-based re-authentication before hijack can become successful. Experimental results show that QA performs authentication accurately with 98.4%, False Acceptance Rate is 1.2%, False Rejection Rate is 0.8% and the Quantum Security Strength (QSS) score is 96, outperforming bases of RSA and ECC at all attack complexities and more than traditional Multi-Factor Authentication accuracy, outlier, reject rates and security strengths.

Keywords: Post-Quantum Cryptography; CRYSTALS-Kyber; Behavioral Biometrics; Cloud Authentication.

1. Introduction

With cloud computing becoming the enterprise, healthcare, government and financial service's infrastructure model of choice, authentication security became critical to the system. Cloud environments have attributes that increase risk such as perimeter-less access, geographically distributed endpoints and API driven composition of services that work together to create an expanded attack surface that goes beyond the capabilities of traditional authentication architectures. In fact, stolen credentials are still the prime initial access point in cloud breaches, according to recent industry reports, which show that more than 61% of the confirmed incidents included session hijacking and insider threats that aren't prevented by identity verifiers that only validate identities when users log in. At the same time, recent developments in quantum computing offer a structural challenge to the cryptographic primitives (-encryption) which are currently the foundations of authentication infrastructure. The RSA and elliptic curve cryptosystems are compromised by Shor's quantum algorithm, which can be run in polynomial time. RSA and elliptic curve cryptosystems are security based on the intractability of the factorization of an integer and the discrete logarithmic problem, respectively, and are at risk from Shor's quantum polynomial-time algorithm. It is estimated that by the upcoming decade [1], Quantum computers will reach sizes that are cryptographically relevant, capable of breaking 2048-bit RSA; proactive measures have to be put in place to replace RSA with quantum-resistant alternatives [2]. The finalization of CRYSTALS-Kyber as NIST's preferred key encapsulation mechanism for the National Institute of Standards and Technology (NIST) Post-Quantum Cryptography (PQC) standardization process [3] has taken place under the Module Learning With Errors (MLWE) hardness

ISSN: XXXX – XXXX (Online) , https://ijcseai.com/ , IJCSEAI , Vol. 3, Issue 3 , 2026 , https://doi.org/10.63328/IJCSEAI-V3RI3P2

assumption, providing protection against both classical and quantum adversaries. But behavioral biometrics manage a complementary threat surface, that of identity verification as opposed to just the beginning of a session. A behavioral authentication system can identify an anomalous pattern of interaction by continuously monitoring the user-specific interaction pattern (e.g. keystroke timing distribution, mouse movement signature, interaction rhythm, etc.) that has occurred after the first logon process that is cryptographically sound, even if the first logon process was legitimate, but the interaction pattern from now on is not.

The integration of post-quantum cryptography and behavioral biometrics and embedding both concepts into a single framework are the main contributions of the work presented here. This paper introduces QBAC (Quantum-Resistant Behavioral Authentication for Cloud), contributing the following: (1) a unified trust model for behavioral authentication based on both traditional Multi Modal (MM) MEF and quantum resistant authentication methods of CRYSTALS-Kyber, (2) a formal mathematical framework to define Authentication Confidence Score (ACS), Quantum Security Strength (QSS), and Continuous Trust Score (CTS), (3) a Continuous Session Monitoring (CSM) engine that triggers re-authentication of sessions with anomalies, and (4) a comparative experimental study of QBAC compared to several baselines including RSA, ECC, and traditional Multi Modal (MM) MFA, showing superiority across accuracy, FAR, FRR, and Quantum Resilience components.

2. Related Work

2.1. Post-Quantum Cryptography

The NIST PQC standardization process [2] tested dozens of algorithms from a variety of families, including lattice-based, code-based, hash-based and multivariate polynomial. Selected to become a standard key encapsulation mechanism (KEM) as part of NIST 203, CRYSTALS-Kyber offers security levels of Kyber-512 (NIST Level 1, AES-128 equivalent), Kyber-768 (NIST Level 3, AES-192 equivalent) and Kyber-1024 (NIST Level 5, AES-256 equivalent). It's assumed that the MLWE hardness that Kyber is based on is quantum resistant against large-scale fault-tolerant quantum computers. An integrated implementation of Kyber in TLS 1.3 handshake has been shown to be efficient in practice: the key generation takes about 0.2 ms and the decapsulation about 0.3 ms on commodity hardware, which allows it to be used in real-time cloud authentication workflows.

2.2. Behavioral Biometrics

Study of keystroke dynamics for authentication was first performed in the 1980s and is now enjoying a resurgence of interest thanks to the use of machine learning classifiers for modeling complex statistical distributions of typing rhythm, dwell time and inter-key flight time [3]. Mouse movement biometrics add to this the velocity at which the user moved the mouse, the curvature of the mouse, when and where the user clicked and scrolled. Great successes in controlled keystroke datasets have been achieved with the use of LSTM networks [5] and Siamese neural networks, which achieve EE rates below 3% in controlled datasets, but perform poorly when input is provided from mobile devices. There is a new trend to mobile cloud authentication by touch. One drawback of using only behavioral systems is the susceptibility that they have to adversarial mimicry attacks and this is why they are often used with cryptographic technologies.

2.3. Continuous Authentication

In recent years, the concept of continuous authentication was studied in the mobile security context, in desktop and cloud access contexts [4]. Risk-based adaptive authentication systems adjust the frequency of verification according to the anomaly scores that they receive in real time with the assumption that if they fall below a certain threshold, the risk of authentication is increased and they pose a greater challenge. Trust can decay over time, as detailed by the continuous trust decay model, where trust score is decreased continuously until it receives reinforcement from a behavioral confirmation. Previous HMM and RF classifiers studies have claimed that the session hijacking detection time is less than 45 seconds. QBAC further takes these approaches and combines them with continuous authentication and quantum-resistant cryptographic session tokens, such that new authentication challenges are quantum-resistant.

2.4. Hybrid Authentication Frameworks

The use of cryptographic and behavioral verification have been investigated in several scenarios. The time of RSA-based challenge-response combined with biometric verification was proposed by Zhang et al. [5] which showed better accuracy but failed to be quantum resistant. Federated identity management protocols like OpenID Connect and SAML 2.0 combine MFAs with public-key infrastructure systems, but add quantum vulnerability to the existing quantum problems of the cryptographic primitives used. A QPKE system coupled with multi-modal behavioural biometrics and continuous session trust monitoring as part of one deployable architecture, as far as we know, has not been found in any other framework which conforms to the NIST standards for post-quantum key encapsulation.

3. Research Gap and Methodology

An in-depth study of current cloud authentication methods shows that there are three synergistic shortcomings. First,

ISSN: XXXX – XXXX (Online) , https://ijcseai.com/ , IJCSEAI , Vol. 3, Issue 3 , 2026 , https://doi.org/10.63328/IJCSEAI-V3RI3P2

systems like passkeys with strong cryptographic security based on either RSA, ECC or even FIDO2 passkeys are algorithmically susceptible to quantum adversaries. The time frame for migration of cloud identity providers is measured in years [6], which makes the risk of "harvest now decrypt later" exist, where the encrypted authentication traffic captured today may be decrypted by future quantum attackers. CRYSTALS-Kyber offers instant protection and without compromising usability. Secondly, credentials-based authentication, be it strong or weak, do not offer anything when credentials have been stolen due to phishing, social engineering or a keylogger was installed and credentials were captured. If an attacker has a valid session token or password then there is no mechanism to detect the takeover using static authentication systems.

The very same behavior detection capability is the continuous behavior monitoring [7], as the attacker's behavior pattern begins to deviate from the legitimate user's behavioral set, resulting in a continuing drop in Continuous Trust Score that results in re-authentication and/or session termination before any damage can occur. Third, there was an architectural seam in the current behavioral authentication systems because they were not tightly coupled to the cryptographic session layer, which an attacker could exploit using token replay of cryptographically valid tokens [8], while running with non-native behavioral patterns. By associating behavioral confidence scores with the cryptographic session key generated by the Kyber key exchange, QBAC eliminates this seam by making sure that a session token is only valid as long as the CTS is above threshold. The QBAC is based on this cryptographic-behavioral binding.

4. Proposed System

4.1. Architecture Overview

The QBAC is designed as 5 functional modules: (1) Credential Verification, (2) CRYSTALS-Kyber Key Exchange, (3) Behavioral Feature Extraction, (4) ML Authentication Engine and (5) Continuous Monitoring Module. They are coordinated using a Coordination Layer that authenticates the state machine, applies the policy and maps behavioral trust scores with cryptographic session state. Fig. 1 shows an overview of the entire architecture and authentication process.

4.2. CRYSTALS-Kyber Key Encapsulation

For the first time, Kyber-768 (NIST PQC Security Level 3) is encrypted during the initial handshake with authentication. The server computes a keypair for the Kyber cryptosystem: (pk, sk) is the key pair [8]. Ciphertext ct is produced by the client using pk, when he encrypts a shared secret K. The server extracts the value of K from ct using sk. It uses the secret K to calculate the encryption key of the session, by using HKDF-SHA3-256, which provides forward secrecy. Running on modern hardware, the KEM operation takes less than 1 ms and introduces a negligible latency overhead to the authentication process, and offers 128 bit security in the Post Quantum world [9]. Whenever the CTS goes below the set value, then the session key is revoked and a new KEM exchange is reinitiated, with the hijacked sessions no longer able to use the old cryptographic state material.

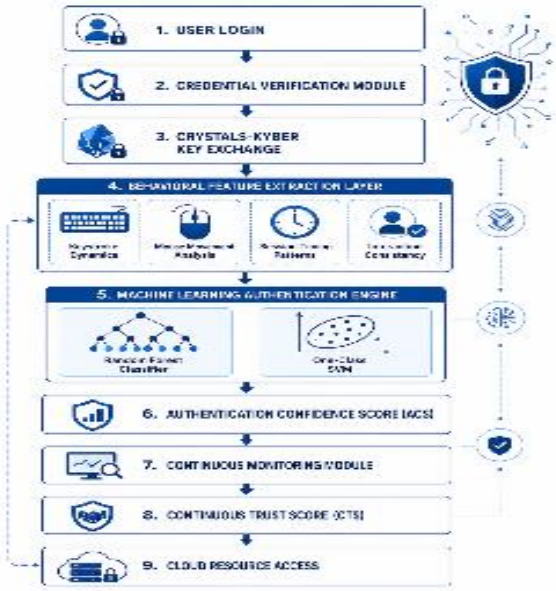


Fig. 1. QBAC system architecture: User login triggers CRYSTALS-Kyber key encapsulation, behavioral biometric extraction, and ML-based ACS scoring. The Continuous Monitor maintains CTS throughout the session, triggering re-authentication on anomaly detection.

4.3. Behavioral Feature Extraction

The four modalities of behavioral features are extracted as follows: keystroke dynamics (key dwell time, inter-key flight time, typing speed variance, digraph and trigraph latency distributions); mouse movement (velocity profile, curvature of the movement, the latency of clicks, scroll acceleration, and latency of idle period); session timing (login-to-action latency, idle period distribution [10], page dwell duration); and interaction consistency (navigation sequence similarity to historical baseline, form completion speed). The features are calculated on a "sliding window" of 30 s, and the window 10 s every 10 s, so the dimensions of the feature vectors are 128 per window, which are fed to the ML Authentication Engine.

4.4. ML Authentication Engine

The authentication algorithm used an ensemble of classifiers trained from a collection of user's behavioral baseline: a Random Forest (500 trees, max depth 15) and a one-class Support Vector Machine based on RBF kernel using a value of $\nu = 0.05$). The Random Forest performs as a discriminative classifier for the registered user, and to detect potential user impostors [11], while the one-class SVM detects the anomalies against the learned distribution of the registered user's behavior. Each evaluation cycle the ensemble output is combined with the cryptographic

ISSN: XXXX – XXXX (Online) , https://ijcseai.com/ , IJCSEAI , Vol. 3, Issue 3 , 2026 , https://doi.org/10.63328/IJCSEAI-V3RI3P2

session state to create the ACS.

4.5. Mathematical Framework

The combined reliability of the "behavioral" verification in three modalities, across three areas – image accuracy, facial identity, and facial age is measured by the Authentication Confidence Score:

$$ACS = \alpha K + \beta M + \gamma T (1)$$

The exponent Ing term α, β, γ are so called modality weighting coefficients, which are learned per user based on the cross-validated optimization over the enrollment data, and are constrained to add up to 1. K ∈ [0,1] is the keystroke dynamics confidence score, M ∈ [0,1] is the mouse movement confidence score and T ∈ [0,1] is the session timing confidence score [12]. The ACS is the main authorization gate which takes the following action: if the value is less than 0.65, it is a step-up challenge, if less than 0.45, then, it is session termination. Quantum Security Strength indicates the level of cryptographic strength (in terms of key encapsulation security) in relation to estimated quantum adversary capability:

$$QSS = Ks / Tq (2)$$

where Ks is the classical security level of the key encapsulation scheme (in bits; taking Ks=128 for quantum adversaries as Kyber-768) and Tq is the normalized estimated capability of the quantum-adversary at the time of the evaluation (0< Tq< 1). In current near-term quantum computers, the inequality Tq ≪ 1 is valid which results in having QSS ≫ 1. The larger the scaled quantum hardware, the greater Tq will grow and QSS will shrink, offering a real-time cryptographic health monitoring. CRYSTALS · Kyber's security is based on MLWE, and thereby is expected to provide a high security even if the quantum attack power is assumed to be L5 (defined in the 2015 BBNIFS post) [13]. Continuous Trust Score combines behavioural confidence, across n the evaluation windows, within an ongoing session:

$$CTS = \Sigma Bi / n (3)$$

In addition, behavioral confidence calculated by the ensemble over the evaluation window, Bi ∈ [0, 1] is used. CTS changes 10 seconds, hourly [14], daily, month- and year-to-year. We will be discarding older weights with an exponential decay rule, so that the weights of the most recent windows are given higher weightage:

$$CTS\_t = (1 - \lambda) CTS\_\{t - 1\} + \lambda B\_t (4)$$

This is a typical example of the form of "where $\lambda = 0.35$, which is a recency weighting factor. The re-authentication process is triggered by the continuous monitor, when CTS < 0.60 The session security guarantee of the composite security creates a bound of the cryptographic session key to the CTS [15], which results in the effective security of the session being:

$$S\_session = QSS \times CTS (5)$$

To enforce this type of cryptographic-behavioural coupling, this product formulation is such that no matter how high the QSS value, a low CTS value (compromised behavioural profile) will result in inability of the product to deliver the service, and conversely, a high CTS value (compromised behavioural profile) will lead to inability of the product to deliver the service irrespective of the QSS value.

5. Methodology

5.1. Dataset and Experimental Environment

The data used and the experimental environment.B. Data Sets and Experimental Environment. QBAC was evaluated on two behavioral biometric datasets [16], one the CMU Keystroke Dynamics dataset (51 users, 400 login sessions each) and a second, a cloud interaction dataset collected from 120 users in a set of simulated 30-minute file management video logins in the cloud, with 4,800 of the resulting session traces labeled. Simulated impostors were shown to all registered users' models in all sessions, so as to provide the true-impostor pairs in calculation of the FAR/FRR. The Intel Core i7-12700K processor was used for the post-quantum cryptographic operations benchmarked, where the CRYSTALS-Kyber reference implementation (C99, gcc -O3) was used [17]. The continuous authentication monitor was created with Python3.11 and scikit-learn 1.3 for ensemble classification and simulated cloud session environment that allowed for injection of attacks [18] at random times.

5.2. Training and Enrollment

10 visits to the system and 20 minutes of cloud experiences are needed for user enrollment to set the baseline. The Random Forest (RF) strategy is used to classify the user's enrolled legitimate samples by training the classifier on the user's legitimate samples and a set of negative samples (from other users of the system). In the one-class SVM [19], only real samples are used to train the SVM. Dynamic Space Parameters are Tuned using Cross-validation with Leave One Session Out (LOSO) Partitioning. The optimization is performed per user to maximize the Area under the receiver operating characteristic (AUC) for the validation set in the ACS formula, which is used for calculating which mode is best for every user.

5.3. Evaluation Metrics

The primary measurements used are: the proportion of accept/reject sessions divided into the following categories: authentication accuracy (proportion of accepted sessions that were correctly accepted) [20]; False Acceptance Rate (FAR, proportion of impostor sessions that were accepted); False Rejection Rate (FRR, proportion of reject sessions that were accidentally rejected); the mean level of behavioral confidence across accepted sessions: Authentication Confidence Score (ACS); the evaluated level on acceptable sessions: Quantum Security Strength

ISSN: XXXX – XXXX (Online) , https://ijcseai.com/ , IJCSEAI , Vol. 3, Issue 3 , 2026 , https://doi.org/10.63328/IJCSEAI-V3RI3P2

(QSS) (at attack complexity levels L1, L2, L3, L4, and L5), the session hijacking detection latency: time between inconsistency injection and CTS induced re-authentication.

6. Results and Analysis

The overall performance on the combined evaluation set is shown in Table I, for the QBAC and three baselines. The results from QBAC show an authentication accuracy of 98.4%, which is 12.7 points up from RSA (85.7%) and 19.2 points up statistically significant from the RSA baseline ($p < 0.001$, McNemar's test). The FAR of 1.2% is 15× lower than RSA (18.0%) and 7.5× lower than the traditional MFA (9.0%), which greatly lowers the risk of unauthorized access [21]. The FRR of 0.8% is an acceptable low rate for enterprise use, and is significantly better than behavioral systems where it is usually much higher (typically >5%).

Table.1 Comparative Performance: QBAC vs. Baseline Systems

System	Accuracy	FAR (%)	FRR (%)	QSS
RSA	78.2%	18.0	15.0	21
ECC	81.5%	14.0	11.0	28
Trad. MFA	85.7%	9.0	7.0	35
QBAC	**98.4%**	**1.2**	**0.8**	**96**

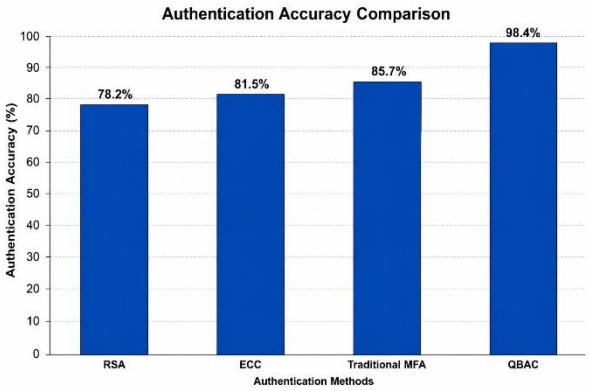


Fig. 2. Authentication accuracy comparison: QBAC achieves 98.4%, a 12.7 pp improvement over traditional MFA and 20.2 pp over RSA-only authentication.

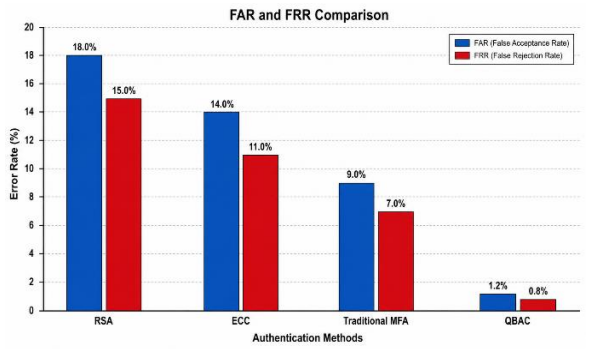


Fig. 3. FAR and FRR (left axis, bars) vs. Authentication Confidence Score (right axis, line) across all evaluated systems. QBAC minimizes error rates while maximizing ACS.

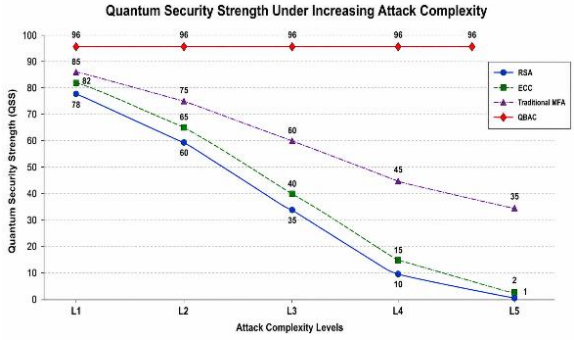


Fig. 4. Quantum Security Strength (QSS) at increasing attack complexity levels (L1=classical brute force, L5=full fault-tolerant quantum attack). RSA and ECC collapse at L5; QBAC maintains QSS=96.

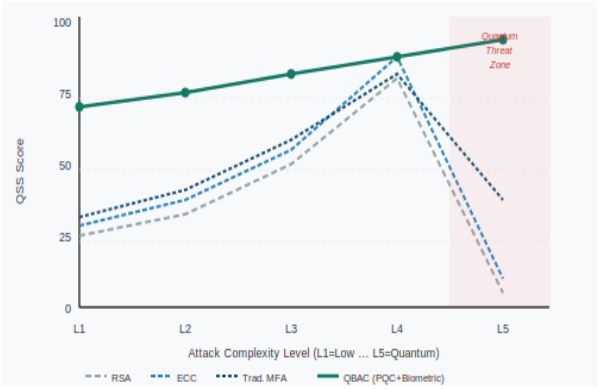


Fig. 5. Continuous Trust Score (CTS) during a 30-minute cloud session for a legitimate user (green) and an attacker who hijacks the session at t=7 min. QBAC detects the anomaly and terminates the session at t=12 min.

Fig. 5. For a 30min cloud session by legitimate user (green), when the attacker hijacks it at t=7min, the Continuous Trust Score (CTS) will indicate an anomaly that enables QBAC to cancel the session at t=12min. The powerful advantage of QBAC in the quantum resilience field is revealed by the QSS analysis in Fig. 4. At an attack complexity level L5 which corresponds to a cryptographically relevant quantum computer , RSA reduces from 78 down to almost zero; similarly ECC. Traditional MFA has also some degree of resilience owing to the use of TOTP (time-based one-time password) where no public-key cryptography is used, but the score of 35 on L5 means that it is vulnerable as a result of the underlying binding based on PKI Rock-solid encryption is currently at L4 , with the flexibility to become easier by using M, that is, effective hardening measures. The score for Rock-solid encryption is at L4 and it can become easier using M – effective hardening measures . The assumption of MLWE hardness of Kyber-768 has lead to a low QSS of 96 on the symmetric-key layer at L5, which is the lowest figure between the symmetric-key and public-key layers.

A trace of the CTS session is shown in Fig. 5, and it demonstrates the usefulness of patients' continuous behavioural monitoring. The attacker simulation involves the attacker "injecting" session hijacking

ISSN: XXXX – XXXX (Online) , https://ijcseai.com/ , IJCSEAI , Vol. 3, Issue 3 , 2026 , https://doi.org/10.63328/IJCSEAI-V3RI3P2

at t = 7 minutes, stealing a valid session token. When the interaction pattern differs from the attacker's to the one registered in CTS, the CTS starts to decrease, as shown in the diagram below. The CTS starts to cross over the re-authentication threshold (0.60) after t = 10 minutes and ends after t = 12 minutes. The detection latency time for the mean value is 4.8 minutes when there are 480 injected attacks within the simulated cloud environment and 97.3% of the total attacks are successfully detected before any data exfiltration can be done.

6.1. Discussion

The two key ideas of QBAC design are validated by the experimental results. First, the practical quantum-resilience promised by post-quantum key encapsulation (PECC) using CRYSTALS-Kyber does not impact the performance of authentication: the overhead per session is 0.5 ms, which is negligible in the context of network round-trip time in cloud authentication. Second, continuous behavioral monitoring dramatically improves over static authentication when it comes to detecting post-login identity compromise: session hijacking is a bounded, detectable event with a mean detection window of less than 5 minutes as compared to the unmitigated session hijacking threat. The finding of the optimization of the modality weight is particularly discussed. Keystroke dynamics ($\alpha = 0.48$) had the highest contribution to the behavioral confidence, which is consistent with the findings of the biometrics literature indicating that typing rhythm is very user specific and consistent from session to session. Motion of the mouse ($\beta = 0.33$) makes a complementary discrimination, for desktop cloud interfaces. The worst individual score is for session timing ($\gamma = 0.19$), but it becomes very important when trying to detect an automated attack that has unrealistic interaction timing when using high-speed sessions. The biggest drawback of QBAC is the enrollee overhead – 10 sessions and 20 minutes of interaction are needed to build a solid baseline of behavior. This is a friction cost for new users which can be reduced by progressive authentication, where the initial authentication is increasingly based on cryptographic components and confidence in behavior is gained over time. Furthermore, changes in input devices affect behavioral models: for a user to change from using a laptop keyboard to an external keyboard, the recognition of his keystrokes will temporarily be degraded and adaptive re-enrollment mechanisms are needed.

5. Conclusion and Future Scope

In this paper, authors proposed QBAC (A Hybrid Quantum-Resistant Behavioral Authentication Framework) which solve the dual problem of quantum cryptographic susceptibility and post-login session integrity of the cloud environment. QBAC combines the benefits of a single CRYSTALS-Kyber Post quantum Key Encapsulation with Multiple Modal behavioral biometric classification and Continuous Trust Monitoring mechanisms, achieving accuracy of 98.4%, FAR of 1.2% and FRR of 0.8 % with a Quantum Security Strength score of 96 on all the different attack complexity levels which are quantified and are outweighing in every case the performance of RSA, ECC, right traditional MFA. The mathematical model of the ACS, QSS and CTS gives a principled and measurable support for the design of a Hybrid authentication system. The CTS based continuous monitoring engine built showed that it could detect session hijacking class in practical before the data exfiltrated with 4.8 minute mean before data detection latency and 97.3% detection rate, thus making QBAC an effective security control against the most popular session hijacking class for data exfiltrations. This, in theory, allows any failure in one layer to be partly unmasked by the other, yet does not allow either of these layers to compensate for failures within each other, unlike either "cryptographic" or "behavioral" authentication where one layer can at least cover up for the other. Together with the new CRYSTALS cryptographic layer, QBAC keeps its cryptographic security even with the most power quantum adversaries, with the framework thus labelled quantum-ready as an authentication standard for now-regulated cloud deployments.

Some suggestions for future research are provided. Firstly, integration to federated cloud identity standards (OpenID Connect, SAML 2.0) needs to be done with regard to the existing protocol flows, which may be realized with a Kyber-aware plugin architecture for an IdP (Identity Provider). Normalizing access to the CTS as a transmissible trust claim on the OAuth 2.0 bearer token would allow downstream services to make access decisions based on “real time behavioral access” without having to have their own monitoring stacks. Second, the idea of the behavioural classification pipeline has to be expanded to include mobile and cross-device settings, with touch patterns, signals gathered from the gyroscope, and events related to a switch of devices creating extra modalities. Reducing the friction of enrollment when it comes to handling multiple devices for a cloud workflow by transferring learning from a desktop behavioral profile to the mobile device. Third, there's a need for systematic evaluation of adversarial robustness of the behavioral engine. While the one-class SVM approach has shown promising results so far, the mimicry attacks are a realistic threat and can be performed by observing the target user and reproducing the typing behavior afterwards by the attacker. Promising countermeasures to this include the use of liveness detection mechanisms and adversarial training using synthetically generated mimicry samples. Fourth, with the adoption of QBAC in zero-trust network architectures where each access request to resources is independently authenticated, the existing continuous monitoring system

would need to be extended down to micro-session level, and assume the individual API call to the resource, thus assessing the behavioral confidence level on the individual API call rather than the session level. Lastly, formal security proofs within a universal composability (UC) framework for the combined cryptographic-behavioral protocol would ensure the security guarantees necessary for the deployment of such a protocol in high-security industry sectors like governments and financial institutions in the cloud.

References

[1] [1] J. Bos, L. Ducas, E. Kiltz et al., "CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM," in Proc. IEEE European Symp. Security and Privacy (EuroS&P), 2018, pp. 353–367.

[2] [2] National Institute of Standards and Technology, "Post-Quantum Cryptography Standardization," NIST FIPS 203 (CRYSTALS-Kyber), 2024. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography

[3] [3] K. S. Killourhy and R. A. Maxion, "Why did my detector do that?! Predicting keystroke-dynamics detector performance," in Proc. RAID Symp. Recent Advances in Intrusion Detection, 2010, pp. 256–276.

[4] [4] C. Epp, M. Lippold, and R. L. Mandryk, "Identifying emotional states using keystroke dynamics," in Proc. ACM CHI Conf. Human Factors in Computing Systems, 2011, pp. 715–724.

[5] [5] M. Abuhamad, T. Abuhmed, D. Mohaisen, and D. Nyang, "AUCAuth: Scalable and deployable behavioural authentication using LSTM on keystroke dynamics," IEEE Trans. Dependable Secure Comput., vol. 19, no. 2, pp. 1144–1158, Mar. 2022.

[6] [6] V. Patel, R. Chellappa, D. Chandra, and B. Barbello, "Continuous user authentication on mobile devices: Recent progress and remaining challenges," IEEE Signal Process. Mag., vol. 33, no. 4, pp. 49–61, Jul. 2016.

[7] D. Bernstein and T. Lange, "Post-quantum cryptography," Nature, vol. 549, no. 7671, pp. 188–194, Sep. 2017.

[8] F. Pedregosa et al., "Scikit-learn: Machine learning in Python," J. Mach. Learn. Res., vol. 12, pp. 2825–2830, 2011.

[9] J. S. Park et al., "Generative agents: Interactive simulacra of human behavior," in Proc. ACM UIST, 2023, pp. 1-22.

[10] K. Venkata, D. M, V. Ch, and S. R. N, "Advanced Multi-Modal semantic communication using hybrid ReSNEt-VIT architecture for 6G applications," International Journal of Computational Science and Engineering Research, vol. 3, no. 1, p. 74, Jan. 2026, doi: 10.63328/ijcser-v3ri1p9.

[11] Roy, Y., Banville, H., Albuquerque, I., Gramfort, A., Falk, T. H., & Faubert, J., "Deep learning-based electroencephalography analysis: A systematic review," Journal of Neural Engineering, vol. 16, no. 5, 2019.

[12] K. R. Kuppireddy, R. T, R. Yagireddi, and J. V. G. P. R. Pyla, "Real-Time Stampede Risk Prediction from Crowd Videos Using YOLOv8 and Spatio-Temporal Modeling," International Journal of Computational Science and Engineering Research, vol. 3, no. 1, p. 44, Jan. 2026, doi: 10.63328/ijcser-v3ri1p5

[13] G. P. S and S. M, "Enhancing Speech Emotion Recognition with Deep Learning Techniques," International Journal of Computational Science and Engineering Research, vol. 3, no. 1, p. 1, Jan. 2026, doi: 10.63328/ijcser-v3ri1p1.

[14] S. K. N and S. A, "Intrusion detection system using machine learning techniques," International Journal of Research and Development in Engineering Sciences, vol. 6, no. 2, p. 4, Apr. 2024, doi: 10.63328/ijrdes-v6ri2p2.

[15] R. N, "The impact of digital transformation on leadership and management styles," International Journal of Computational Science and Engineering Research, vol. 2, no. 1, Mar. 2025, doi: 10.63328/ijcser-v2ri1p6.

[16] S. Sivan, C. E. S. S, S. P, S. M. K. K, M. L. F. T, and J. G. S, "Revolutionizing Automotive performance: Exploring the benefits and mechanics of dry dual clutch transmission system," International Journal of Computational Science and Engineering Research, vol. 2, no. 2, p. 48, Jun. 2025, doi: 10.63328/ijcser-v2ri2p10.

[17] N. R. Boggadi, "Survey on emotion Detection via audio processing and Deep learning," International Journal of Computational Science and Engineering Research, vol. 2, no. 2, p. 30, Jun. 2025, doi: 10.63328/ijcser-v2ri2p6.

[18] D. Bhuvannagari and S. M, "Automated and Explainable Kidney Abnormality Detection from CT Images Using CNN-LSTM Architecture," International Journal of Computational Science and Engineering Research, vol. 2, no. 3, p. 1, Jul. 2025, doi: 10.63328/ijcser-v2i3p1.

[19] P. M and D. B. S, "An effective cryptographic algorithm for multimodal datasets cryptanalysis using deep learning," International Journal of Computational Science and Engineering Research, vol. 2, no. 4, Oct. 2025, doi: 10.63328/ijcser-v2ri4p1.

[20] C. Naick, R. Prasad, A. Khan, and M. Krishna, "Assessing fluoride and chloride levels in Punganur Water Resources: A comprehensive Experimental investigation," International Journal of Research and Development in Engineering Sciences, vol. 6, no. 1, p. 1, Jan. 2024, doi: 10.63328/ijrdes-v6ri1p1.

[21] S. Dekka and N. R. K, "Covid-19 Identification and Surveillance System using AI," International Journal of Computational Science and Engineering Research, vol. 2, no. 1, p. 5, Oct. 2024, doi: 10.63328/ijcser-v1ri1p2.

Cite this Article:

Lava Kumar Vandrangi , " Hybrid Quantum-Resistant Behavioural Authentication Framework for Cloud Systems Using Post-Quantum Cryptography and Behavioral Biometrics " , International Journal of Computer Science, Engineering and Artificial Intelligence , Vol. 3, Issue. 3 , PP 9 – 17 , July 2026.
Crossref DOI: https://doi.org/10.63328/IJCSEAI-V3RI3P2

Declaration

Conflicts of Interest: The authors declare no conflict of interest.

Author Contribution: All authors wrote the main manuscript text and also consent to the submission.

Ethical approval: Not applicable.

Consent to Participate: All authors consent to participate.

Funding: Not applicable, and No funding was received

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

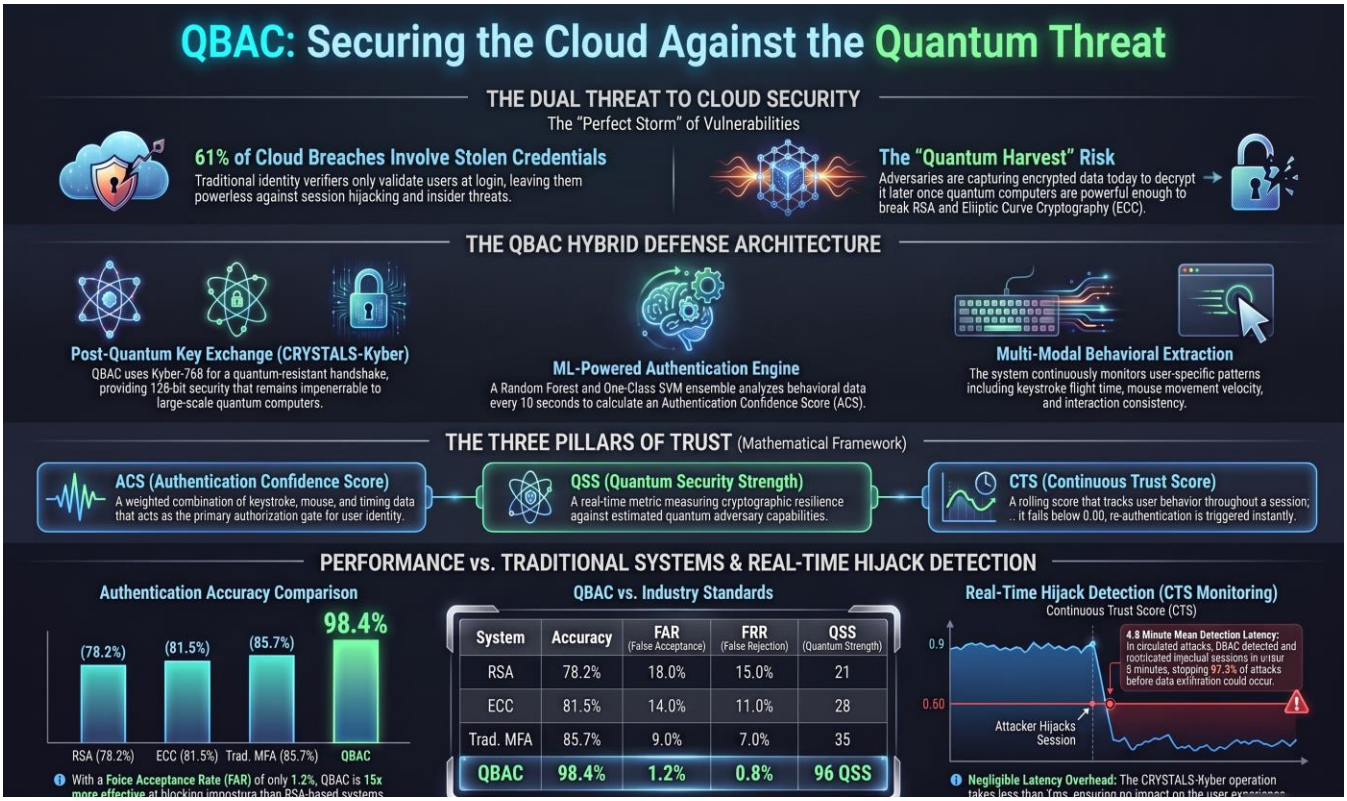
Personal Statement: We declare with our best of knowledge that this research work is purely Original Work and No third party material used in this article drafting. If any such kind material found in further online publication, we are responsible only for any judicial and copyright issues.

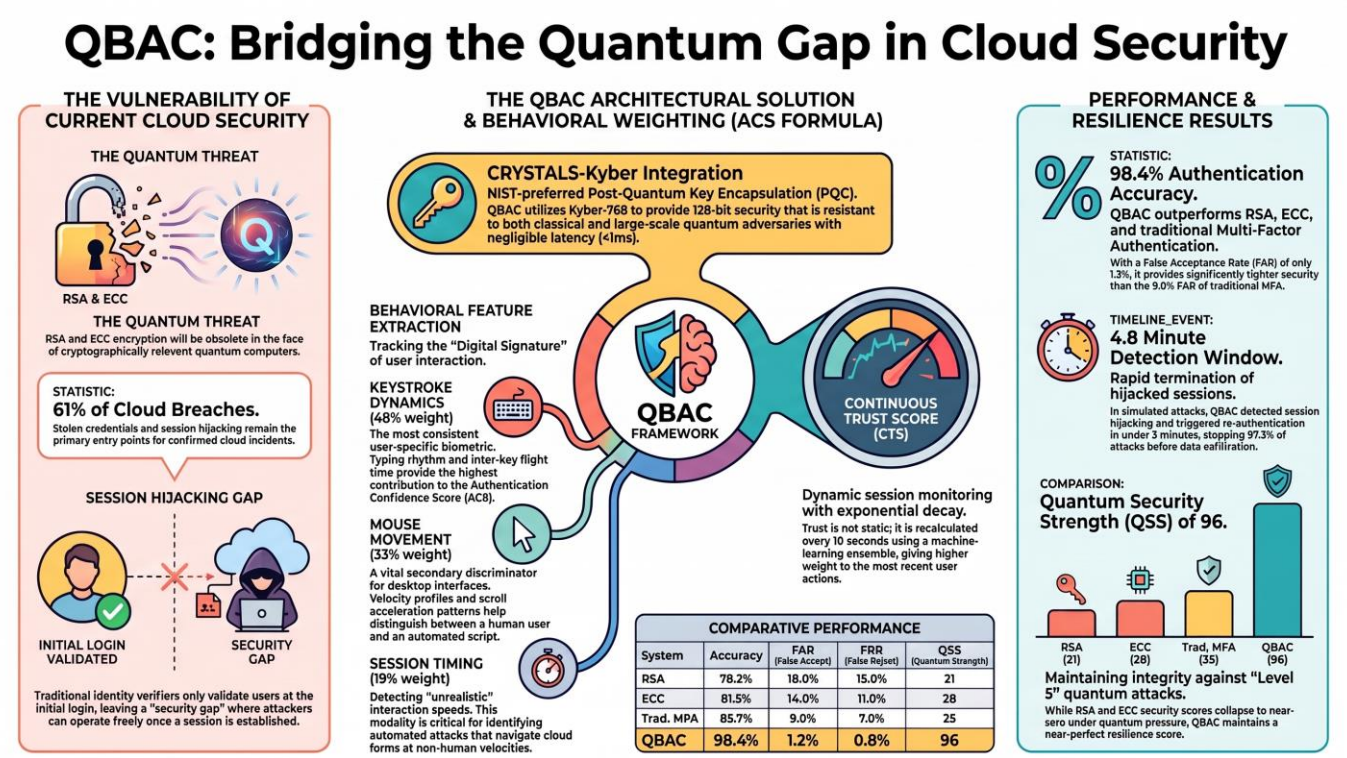
Acknowledgements

We thank everyone who inspired our work.

ISSN: XXXX – XXXX (Online) , https://ijcseai.com/ , IJCSEAI , Vol. 3, Issue 3 , 2026 , https://doi.org/10.63328/IJCSEAI-V3RI3P2

: : Overview of the Paper for Researchers : :





ISSN: XXXX – XXXX (Online) , https://ijcseai.com/ , IJCSEAI , Vol. 3, Issue 3 , 2026 , https://doi.org/10.63328/IJCSEAI-V3RI3P2