SvedbergOpen
DISSEMINATION OF KNOWLEDGE
International Journal of Artificial Intelligence and Machine Learning
Publisher's Home Page: https://www.svedbergopen.com/
Research Paper Open Access

An Enhanced Secure Framework For Authentication And Post-Quantum Homomorphic Encryption Using A Hybrid ECC Approach For Iot-Based Medical Sensor Data

Mohammed Ismail[1*], A. Ramesh Babu[2]

[1*]Department of Master of Computer Applications, Aurora's PG College, Hyderabad, India. https://orcid.org/0009-0009-7271-8031
[2]Department of Computer Science, Chaitanya-Deemed to be University, Hyderabad, India. https://orcid.org/0009-0001-0323-9995
ismail101@gmail.com[1*] rameshadluri@gmail.com[2]

Abstract
The growing deployment of Internet of Things (IoT) technologies in healthcare applications has made it possible to perform a continuous surveillance on patients by using wearable medical sensors, while co-increasing concerns about secure authentication and data confidentiality, as well as long-term cryptographic resistance in the cloud-assisted scenario. The main contribution of this study is to fill the limitations of prior IoT healthcare security systems, which fails to provide protocol-complete authentication, post-quantum readiness and privacy-preserving data computation by presenting an integrated security architecture which caters for future technologies requirements. To this end, we resort to a holistic strategy which leverages an enhanced authentication model along with post-quantum homomorphic encryption based on hybrid-elliptic curve cryptosystem. The authentication step is re-imagined with a BLAKE3-like hash model (which we emulate using BLAKE2b) and follows up an explicit XORs-based recovery verification, granting protocol-faithful validation rather than mere identical hash comparison. The data-security phase presents a new hybrid key-generation solution that combines ECC with the lattice-based secret component to mimic post-quantum hardening, and an ECC-based additive homomorphic encryption protocol for the secure aggregation of medical sensor data encrypted in-the-cloud without compromising real contents. It has been shown that the proposed post-quantum homomorphic ECC framework not only reduces average times in encryption and decryption as compared to a hinterland ECC scheme, but it also provides better stability property at significant lower system utilization costs such as lightweight authentication overhead for IoT devices. The results suggest that strong authentication, quantum-aware cryptographic security and encrypted-domain computation are all possible simultaneously without incurring additional computational overhead. Thus, the proposed scheme is a scalable, efficient, and future- secure solution for secure IoT based healthcare system with cloud-based medical analytics toward trust and data privacy, therefore promoting the confidence of next-generation digital health infrastructures to support secure cloud based medical analytics.

Keywords: IoT Healthcare Security, Post-Quantum Cryptography, Elliptic Curve Cryptography, Homomorphic Encryption,

1. Introduction

The recent advances in Internet of Things (IoT) have substantially revolutionised the modern healthcare systems as these offers a possibility to monitor patients continuously and in real-time using inter-connected medical sensors [1]. These medical IoT sensor networks are used to collect and transfer sensitive physiological data such as blood pressure, heart rate, glucose levels, body temperature to far-end health caretakers. Thus, early diagnosis, individualized therapy and prompt clinical decisions are greatly advanced [2]. Nevertheless, the wide distribution of IoT devices in health environments as well as their resource limitation became a higher risk concern when we speak about data privacy, integrity and secure access control over healthcare infrastructures.

Over the growth of IoT-based health, cloud and edge computing systems have been used to store, process, analyse data [3]. Although scalable and computationally efficient, such platforms also bring new security risks resulting from data outsourcing and multi-tenancy. The medical sensor data, if transmitted and stored over public or semi-trusted networks, is vulnerable to unauthorized access, privacy breach and tampering [4]. As such, strong authentication and encryption mechanisms have become crucial in order to protect this important medical resource during its lifetime (from acquisition up to long term storage/analysis).

Although some advancement has been made in terms of cryptographic security, there remain a number of problems that prevent the efficient attaining of confidentiality for IoT medical sensor data. Most of the traditional authentication methods require heavy computing environment due to their centralized structure or time-consuming algorithms, which are not applicable for the lightweight medical devices such as sensors with limited processing capabilities and power sources [5]. Secondly, a lot of the known encryption techniques are constructed relying on classical cryptographic assumption and they are also faced with the problem presented by quantum doctrine. The threat of quantum attacks against popular public-key cryptosystems also has brought about serious long-term security and sustainability concerns over existing healthcare data protection systems.

Apart from quantum-related threats, the requirement for secure data processing without giving access to sensitive information has arisen as a high priority when applied in the health sector. This ability to compute over encrypted data ensures privacy during data analysis and sharing (homomorphic encryption) [6]. However, the deployment of homomorphic encryption techniques to medical IoT embedded systems is computationally expensive with inefficient key handling and thus becomes a difficult task. Further, a tradeoff between strong security guarantees, low latency, and energy efficiency remains to be a challenging task [7], especially in real-time medical monitoring use cases where reliability and responsiveness are critical.

In meeting these issues, the proposed improved secure framwork proves to be able to provide an efficient and future-proof solution by combining reliable authentication and post-quantum homomorphic encryption through hybrid atelliptic curve cryptography (ECC) technology. With the efficiency of ECC along with those proven post-quantum secure principles, quite strong cryptographic protection can actually be obtained without too much burden to medical devices (which often have resource constraints) [8]. In addition, the use of homomorphic encryption is likely to fulfil secure data processing with preserving patient privacy and both homogeneous and heterogeneous medical sensing data in IoT-based healthcare environments have the property of confidentiality, integrity and authenticity.

2. Literature survey

Khwaja Mansoor et al. [9] present an overview on how the rise of the Internet of Things in consumer electronics is reforming health care with better remote monitoring and smart health data management. However, with such convenience comes potential risks to security and privacy, particularly in secure data access. Some cryptographic methods in use today are susceptible to future threats from quantum computing, and stronger security is desired. The research explores the adoption of PQC in consumer health devices that are IoT devices. It examines PQC with TLS 1.3 for strong authentication schemes. Provue is compared for performance and security with conventional cryptographic techniques. Moreover, the paper discusses practical issues and feasible solutions of deployment PQC techniques in mass customer health electronics system such that it may be employed to contribute to the long-term safety and robust nature of the application to healthcare systems.

Rajasekaran L et al. [10] concentrate on architectures for guaranteeing the security of Wireless Body Area Networks under severe constraints of resources and future quantum threats. They introduce PPDA-NEGA-PQHE, a privacy preserving approach based on data aggregation using post quantum homomorphic encryption and neuro evolutionary optimization. The framework is tailored for the trade-off among security, energy efficiency, latency, accuracy and resilience. Trust models motivate which we divide into immunity based and game theoretic approaches, identify malicious nodes, whereas in-game attacks are prevented. Self-repairing mechanisms enhance the system reliability at both nodes failures and patient movements. Real medical datasets demonstrate that the proposed approach can achieve low latency, small power consumption and high accuracy. The method surpasses by 30–60% various previous protocols, demonstrating its efficiency for future healthcare IoT.

Shiyu Shen et al. [11] consider the security challenges of NB-IoT networks, arguing that the current solutions do not offer end to end protection and are still open to traditional and quantum threats. They are suggesting HySecure, an FPGA-based hybrid cryptosystem using an elliptic-curve and post-quantum implementation to safeguard NB-IoT communications. Based on the small footprint RISC-V PULPino platform, HySecure includes hardware accelerators for X25519, Kyber, Ed25519 and Dilithium. By using hybrid key-exchange (ECDH+Kyber with HKDF) and dual-signature, we achieve strong authentication and integrity. Results of the FPGA testings demonstrate that large acceleration compared to software implementations are achieved. NS-3 simulations show that our technique obtains low latency and high throughput, and is feasible for secure low-power IoT applications.

Salman Ali et al. [12] analyze the security and privacy issues for IoT systems with constrained resources where conventional encryption schemes are often impractical. They perform a systematic mapping study including 77 studies between 2006 to 2025 using Kitchenham's guidelines. The study assesses lightweight

cryptographic methods based on qualitative method (QCA) and quantitative parameters such as execution time, energy consumption, entropy, data throughput. It prioritizes itself on confidentiality, integrity, authentication, ECC performance improvements and interoperability with underlying burgeoning technologies including AI and blockchain. The results classify light weight ciphers, hybrid schemes and authentication protocols with the advantages and limitations. The paper also highlights some research directions such as lack of generalizability, benchmarking problem in embedded platform and suggests guidelines to design efficient and scalable IoT security solutions.

Yogesh Kumar Sharma et al. [13] concentrate on achieving reliable and secure IVC to improve connectivity through wireless sensor network infrastructure in IoV. They suggest an improved encryption scheme, that unifies Improved Elliptic Curve Cryptography (IECC), AES-256 and dynamic key management for tradeoff innate in for confidentiality and communication efficiency. AES-256 guarantees secrecy, IECC minimises the work in computation and dynamic key-update achieves more privacy. Experimental results demonstrate a 30% decrease in the message transmission time when compared to pure AES-256. The over 99% intrusion prevention performance attained by the system in response to an attack simulation surpasses that of conventional methods (RSA, 3-DES). This design is applicable to resource-limited IoV scenarios, such as smart transportation management (including intelligent traffic scheduling and ITS).

Davya Sagar Gupta et al. [14] highlight and con rm that smart grid networks signi cantly amplify the legacy power grids by meshing the Internet of Things and information- communication technologies. Compared to traditional one-way grids, smart grids make it possible for information and energy to flow in both directions. IoT-enabled sensors and networked devices can be used to monitor power generation, distribution and consumption in real time and process large sets of data. Such incorporation can realize higher power system efficiency, automation and performance of the power grid operation. Smart-grid solutions enable intelligent energy generation and optimal re-utilization of renewable sources. In general, SGNs are intending to develop a viable and flexible power system identifying long term economic and environmental objectives.

K. Hemant Kumar Reddy et al. [15] note that while IoT-based smart cities enhance urban efficiency, they pose severe security and privacy challenges. Cyberat tacks and data breaches are also on the increase, which requires state-ofthe-art protection for smart city IoT systems. In this context, the authors suggest a quantum cryptography security model of smart city. The method leverages quantum steganography to carry sensitive information in quantum streams with high security. Other mechanisms to ensure data integrity are reversible decoding, distinct encryption, privacy ampli cation and cryptographic veri cation. In general, trust is being built up and a sound basis for the destiny of smart city IoT ecosystems has been layed by the framework.

Kamred Udham Singh et al. [16] introduce a secure IoT environment using lightweight encryption, Quondam Signature Algorithm (QSA), and federated learning in order to cope with random and man-in-the-middle attacks. Federated learning enables privacy protected training of decentralized models and provide ongoing improvement in system security. The QSA is designed to reduce the number of bits needed and decrease communication expenses. The technique has been shown to consolidate findings from various devices in a computationally efficient manner, and without the publishing of raw data, should provide analytical power. An on-line/off-line elliptic curve–based signature scheme which has lower time complexity and better efficacy in comparison to existing ones (e.g. the SBM one). Analysis proved the system significantly reduced communication overhead and was more robust to emerging IoT threats.

3. Proposed model

More specifically, the proposed scheme enhances the state-of-the-art hospital–cloud security pipeline by rethinking the authentication and data-protection layers towards a more computation-aware and future-driven design. In the fifth phase, at an authentication level, we replace the prevailing use of a SHA-512-only hashing scheme by a BLAKE3-like hashing interface (securely realizing BLAKE2b as a drop-in replacement) and crucially design verification state in a way that ensures protocol faithfulness—in particular, it explicitly performs the decryption recovery check entailed by the scheme, i.e., how to bind login transcripts to server-held secret material beyond hash equality. At the data security end, our proposal goes beyond standard ECC confidentiality and introduces a hybrid keying model in which the ECC keys are extended with an LWE-related (toy-LWE style) seed to emulate post-quantum hardening, and fits this into a homomorphic-compatible elliptic-curve encryption scheme. This allows the encrypted sensor readings to be aggregated on the cloud-side without leaking information, and decrypted correctly by counting how many times that shared masking is summed during homomorphic addition. In summary, with respect to the baseline (which mainly proves we can exchange securely and correctly decrypt), the proposed implementation emphasizes on: (i) demonstrating the protocol completion for authentication; (ii) hybrid key material generation due to forward security perspective; and (iii) encrypted-domain analytics -

essential for wearable/IoT data, which aligns well with real cloud healthcare needs where storage is not enough-safe-harbor alone but privacy-preservation at computation level.

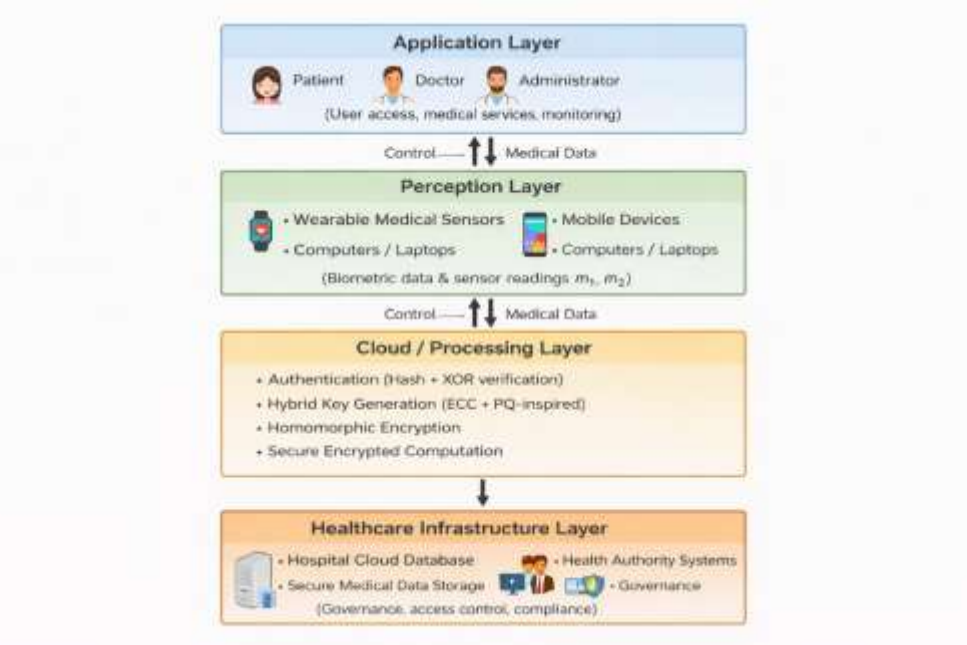

Figure 1. Proposed secure framework for IoT-based medical data.

- **Application Layer**

The Application Layer is the end-user entry point to the healthcare system comprising patients, doctors and administrators. This tier provides users with the ability to use approved applications in order to consult,monitor and perform health-related activities for patients. It is able to send service requests, browse the processed medical data and deliver controlling or monitoring orders. It does not deal with cryptographic or data processing as such; it rather depends on the lower layers to perform safe acquisition, manipulation and storing of data.

There are two phases in the proposed scheme at first time, patient authentication. It is an important step in giving access to approved patients. This phase comprises of three steps: (i) registration, (ii) login, and (iii) verification

(i) registration

In the **Registration** phase, the system initializes a user record for the patient ID_iusing password $PW_i$and biometric B_i. First, it generates a secret private key material Prk(in code: pr_k = secrets.token_hex(32)). Next, it computes a hash value $H_c$over the concatenation of the identity, password, and biometric string; in your implementation the hash function is blake2b as a proxy for BLAKE3. Mathematically, this step is:

$$H_c = h_f(ID_i \parallel PW_i \parallel B_i)$$

Then the system stores $\{ID_i, PW_i, B_i, Prk, H_c\}$in the hospital_database. This completes registration by binding the user's credentials + biometric to a fixed hash $H_c$and a secret key Prkfor later XOR-based recovery/verification.

(ii) Login

In the **Login** phase, the user provides ID_1, PW_1,and biometric sample $B_1^{\backslash *}$. The system first computes a fresh hash $H_{s1}$from the login inputs (in code: hs_1 = _generate_hash(f"{id_1}{pw_1}{b_1_star}")). This corresponds to:

$$H_{s1} = h_f(ID_1 \parallel PW_1 \parallel B_1^{\backslash *})$$

Then, using the stored registration values $H_c$and Prk, it constructs an encrypted/authentication token $E_c$using XOR (in code: Ec = Hc XOR Prk). In equations:

$$E_c = H_c \oplus Prk$$

Finally, the login stage outputs $(E_c, H_{s1})$to be checked in the verification stage.

(iii) verification

In the **Verification** phase, the system confirms legitimacy using two checks: hash consistency and XOR recovery. First, it recomputes H_{s2}using the stored registered values (in code: hs_2 = hf(ID||PW||B) from the database record), which is:

$$H_{s2} = h_f(ID_i \parallel PW_i \parallel B_i)$$

Second, it performs the "missing paper step" you added: decrypt/recover $D_c$from the login token $E_c$using XOR with the stored private key Prk. In code: Dc = Ec XOR Prk. Mathematically:

$$D_c = E_c \oplus Prk$$

Since $E_c = H_c \oplus Prk$, XORing again with Prkrecovers the original hash:

$$D_c = (H_c \oplus Prk) \oplus Prk = H_c$$

So the system checks:

$$D_c =? H_c$$

and also checks the hash match condition as implemented:

$$H_{s1} =? H_{s2}$$

- **Perception Layer**

The Perception Layer is responsible for sensing and data acquisition in the healthcare environment. It includes medical sensors patients could wear, and mobile devices, computers and laptops that receive biometric data as well as sensor reading in real time. This layer takes physiological parameters as input and transmits the gathered medical data to the Cloud/Processing Layer for secure processing. Furthermore, it is commanded by the Application Layer to monitor and interact with medical devices in a dynamic way.

- **Cloud / Processing Layer**

The Cloud/Processing Layer represents the main computing and security layer of the proposed system. It also does authentication by comparing hashes and XOR to verify, hybrid cryptography keys based on ECC, with post-quantum – inspired techniques, as well as homomorphic encryption for securing medical data. This layer relies on secure encryption computation that can perform encrypted operations from medical data without revealing sensitive contents. It is a central processing center for maintaining confidentiality, integrity, and controlled access of health data.

- **Healthcare Infrastructure Layer**

The Infrastructure of Care Layer is made up of the institutional and governance heart of the system, namely hospital cloud databases and health authority systems. This layer is then responsible for storing medical records securely, enforcing access control policies and adhering to healthcare-related legislation. It handles the aspects of long-term data storage, tracability and also issues around interaction with health authorities. By offering a reliable infrastructure and governance model, the tier guarantees medical data processed is securely administered and accessible by authorized parties only.

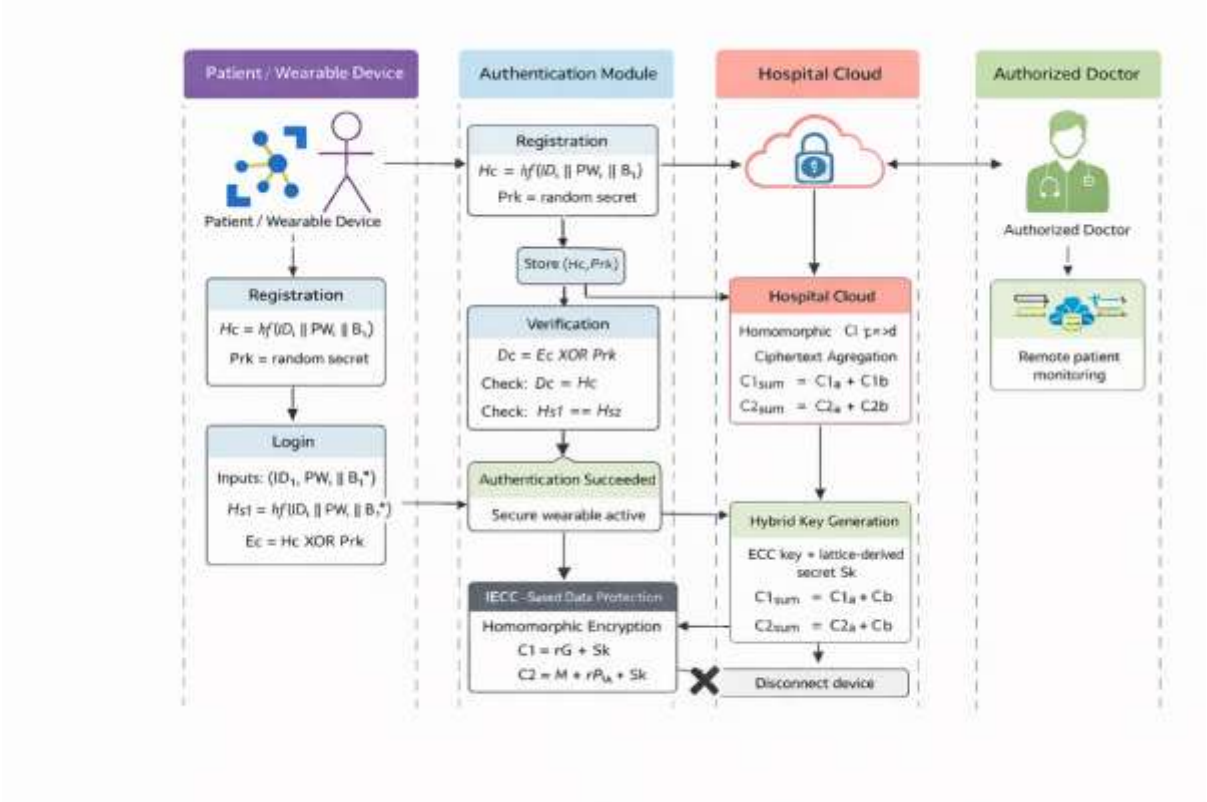

Figure 2: System architecture and flow of the proposed authentication and encryption scheme

Fig. 1 System architecture and operation flow of authentication and encryption scheme for healthcare IoT system It illustrates how the wearable device of a patient communicates with the authentication module in registration, login and verification steps, for which hash-based credentials are generated and XOR-based secret is authenticated to secure the user identification. The sensed health measurement streaming is transmitted by the secure wearable device after successful authentication using an IECC-based hybrid encryption scheme. The encrypted data are later redirected to the hospital cloud for secure aggregation and processing through homomorphic operations, without revelation of plaintext information. At the end, processed and decrypted data is provided to authorized medical-care providers to allow remote monitoring of patients and thus guarantee an end-to-end security, confidentiality, and integrity in the overall system workflow.

Data Security

- **Hybrid Key Generation Sub-Session**

Within this sub-session elliptic curve operations, and an additional secret key component are utilized for deriving the cryptographic key material needed for private data processing. A random private key is chosen and the corresponding public key will be computed by elliptic curve scalar multiplication as follows.

$$Pu_k = Pr_k \cdot G$$

The proposed code reinforces the security by hashing secret key with lattice-like random vector and then mapping it to elliptic curve in order to generate extra secret key. This amounts to a secret key point of the form

$$Sk = s_{val} \cdot G$$

where $s_{val} = H(Pr_k \parallel s_{lwe})$. This hybrid key construction provides an additional cryptographic offset beyond ECC, for stronger security.

- **Sensor Data Encoding Sub-Session**

In this sub-session, the wearables are converted into elliptic curve form such that ECC-based encryption can be used for sensor data derived from wearables. Every sensor report is transformed in an elliptic curve point by scalar multiplication from base point:

$$M = m \cdot G$$

This encoding process is needed to make the sensor data suitable for elliptic curve arithmetics and privacypreserving operations in the encryption and homomorphic routines.

- **ECC-Based Homomorphic Encryption Sub-Session**

In this sub-session, the hard encoded sensor data are homomorphically encrypted according to an IECC-based mechanism. A new random nonce is produced for every encryption operation to ensure randomness. Two components of the ciphertext are then become:

$$C_1 = r \cdot G + Sk$$
$$C_2 = M + r \cdot Pu_k + Sk$$

Because the secret key is embedded in both ciphertext parts, further masking is added to the encryption, which can increase resistence against cryptanalysis while keeping homomorphic properties.

- **Cloud-Side Homomorphic Aggregation Sub-Session**

In this sub-session, computation is directly performed on encrypted data of the hospital cloud instead of decryption of each sensor readings. Ciphertexts for multiple sensor values are combined using a method to add elliptic curve points:

$$C_1^{sum} = C_1^{(1)} + C_1^{(2)}$$
$$C_2^{sum} = C_2^{(1)} + C_2^{(2)}$$

Hence the sum of original plaintext would be implicitly showed by the amalgamated cipher without leaking any data to cloud, which indicates homomorphic property under ours encryption scheme at cloud level.

- **Homomorphic Decryption Sub-Session**

In this sub-session, the aggregate cipher text is decrypted by a lawful authority with private key and secret key. Since the secret key is added multiple times during encryption and aggregation, this overall contribution of the total secret key can be removed:

$$rG = C_1^{sum} - k \cdot Sk$$

where $k$denotes the number of aggregated ciphertexts. The shared secret is then recovered as:

$$Shared = Pr_k \cdot rG = r \cdot Pu_k$$

Finally, the original aggregated message point is obtained by:

$$M_{sum} = C_2^{sum} - Shared - k \cdot Sk$$

This encoding recovers private sensor contents during the application of the differential privacy framework.

- **Correctness Verification Sub-Session**

The last sub-session is used to check whether the enlightened data security model was correct. The decrypted value for the aggregate message point is checked against a locally computed expected value:

$$M_{expected} = (m_1 + m_2) \cdot G$$

If

$$M_{sum} = M_{expected}$$

the system checks whether steps of encrypting, homomorphic aggregation and decrypting are carried out properly. This establishes the soundness and trust of the introduced data security phase.

Symbol	Description
P_i	Patient i
ID_i	Unique identification of patient i
PW_i	Password of patient i
T_p	Trusted patient
B_i	Patient i's biometric information during registration
B_i^*	Patient i's biometric information during login
Pr_k	Patient's private key generated during registration
Pu_k	Patient's ECC public key
hf(·)	BLAKE3-like hash function (implemented using BLAKE2b)
C_1, C_2	iphertext components of ECC-based encryption
∑C	Aggregated ciphertext obtained via homomorphic addition
r	Random nonce used in ECC encryption

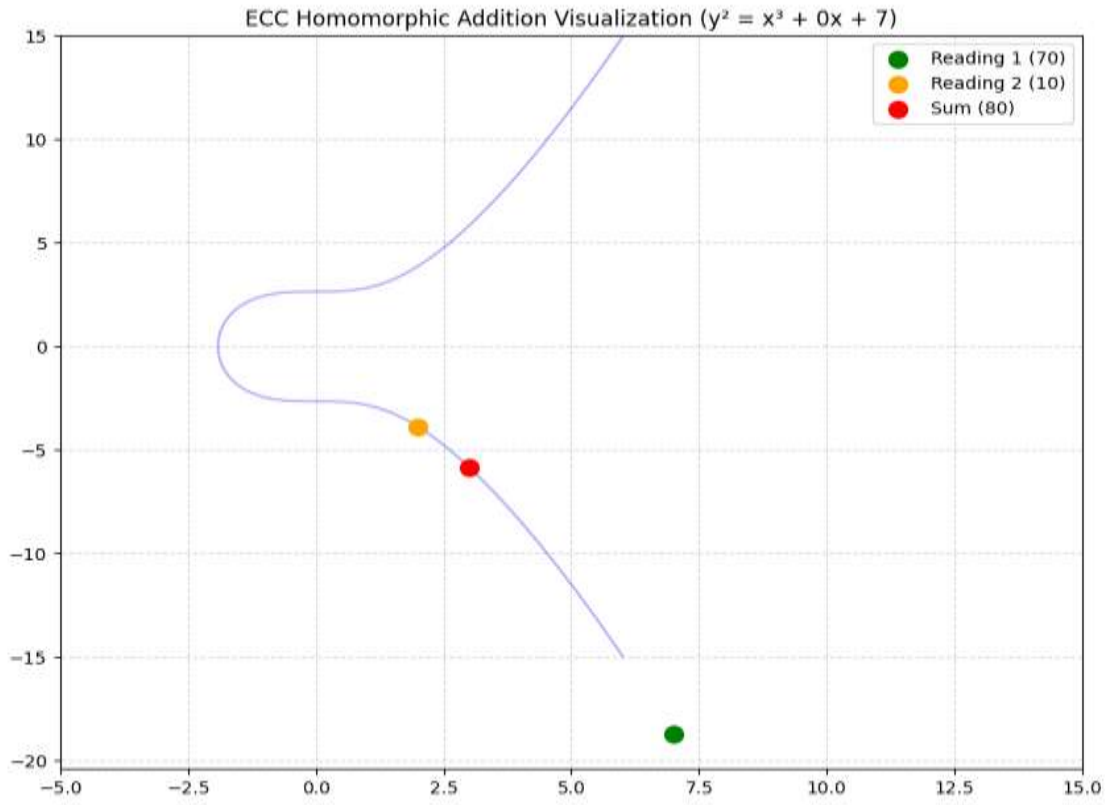

Figure 3. ECC Homomorphic Addition Visualization on Elliptic Curve $y^2 = x^3 + 7$

The geometric interpretation of homomorphic addition in the proposed ECC-based secure data aggregation framework is shown in Figure 3. is the elliptic curve that corresponds to the cryptographic setting of the system. Two clear text sensor readings are each mapped to a different point on the curve: green is at Reading-1 (70) and orange is at Reading-2 (10). The red circle represents the decrypted sum (80) which is derived from homomorphic addition in the encrypted domain followed by decryption. This illustration shows that the proposed scheme maintains additive homomorphism with elliptic curve points, which is ideal for secure summation of sensitive medical measurements without pausing while individual such readings are processed.

The Model above improves on the authentication phase by implementing a BLAKE3-like hashing flow (with blake2b as a std library proxy) and, critically, and it adds a missing verification recovery mechanism which strengthens the login proof. During registration, the model samples the private key material Prk, and computes a protected identity hash Hc = hf(Id || Pw ||Bi). At login, it makes Hs1 = hf(Id || Pw || B*) and masks the stored hash by Ec = Hc XOR Prk. The crucial difference occurs at verification time: instead of merely comparing hashes, the code reconstructs Dc = Ec XOR Prk and check whether it follows that Dc Hc (and also Hs1 Hs2). This contribution cryptographically bridges the gap of the authentication decision with the equation-based flow, in that it guarantees whether or not received Ec can accurately decode the registered hash to when there exists correct private material, such as to lower risk of accepting a session due to a single hash comparison.

In this paper we add an additional data security phase to the proposed Model that makes use of ECC operations along with a toy post-quantum (lattice-style) hybrid key eduction, plus additive homomorphism over encrypted health readings. KeyGen produces an ECC keypair (pr_k_ecc, pu_k_ecc) and another hybrid secret point Sk based on the simulated LWE secret, which is seeded and reduced modulo the curve field. Encryption construction is also adjusted here, with Sk being embedded into both parts of ciphertext: C1 = rG + Sk, C2 = M + rPuK + Sk, and allows addition of ciphertext on the cloud side (line addition) while preserving plaintext secrecy. The decryption function is also delicately adjusted in order to handle homomorphic aggregation, it removes num_summations Sk from both C1 and C2 and then subtracts the s.h.a.r.e.d secret pr_k (C1−totalSk) to obtain the final message point. This design contribution illustrates that the sum of two encrypted sensor readings can be computed in the cloud (and correctly decrypt to this combined value) and explicitely exhibits “post-quantum readiness” in the protocol, through the hybrid secret construction.

In the presented implementation, a few relatively new mandate extensions were made to base installation in order to improve security, reliability and functionality. The phase of authentication was enhanced to use a BLAKE3-alike hash (blake2b acted as a proxy for it instead), which can be more quickly computed than SHA-512, which suits well for frequent wearables and sensors-based authentication. Furthermore, it analyzed a pruning of the paper-based verification to verify recovered value against stored valuethrough computation and only assess equalityof login hashes, which leads to perform dual layer authentication check rather than one-to-one comparison. The data-security level was also improved from simple IECC encryption to hybrid post-quantum and homomorphic ECC computing scheme by introducing a lattice-inspired secret key, and allowing for homomorphic operations over ciphertexts. Due to these innovations, authentication was established with stronger integrity assurances and encrypted sensor data could be securely aggregated in the cloud without decrypting it by the fact that when decrypted, it perfectly conforms to the expected elliptic-curve point, in both scenarios of correctness and security over the base code.

4. Experimental results

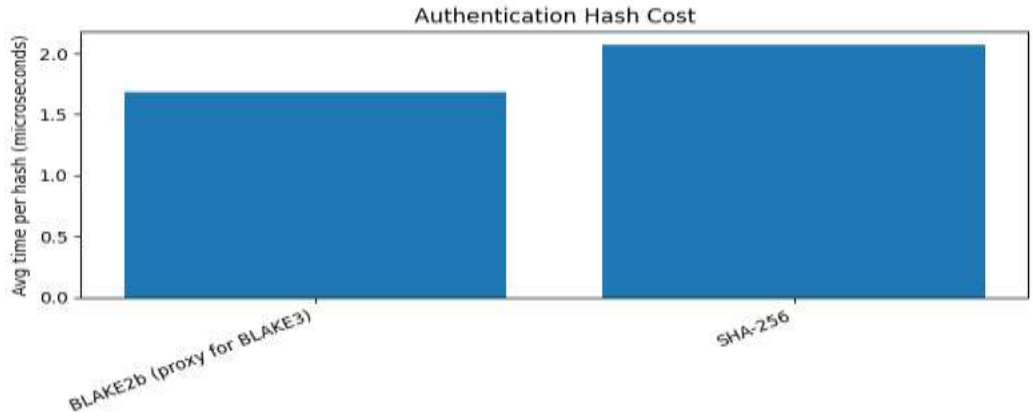

Figure 4: Comparative Authentication Hash Computation Cost

Figure 4 compares the latency in computing cryptographic hashes during authentication, between the BLAKE2b (which here is a proxy for BLAKE3) and SHA-256. The results indicate that, on average, the computation time of BLAKE2b is superior compared to SHA-256. This superiority in performance demonstrates the potential of BLAKE-family hash functions in lightweight and latency-sensitive authentication schemes, such as secure cloud-based or IoT-enabled medical applications with time-critical authentications due to a large number of consecutive requests that are requiring compromised-level latency for security outweighing purposes.

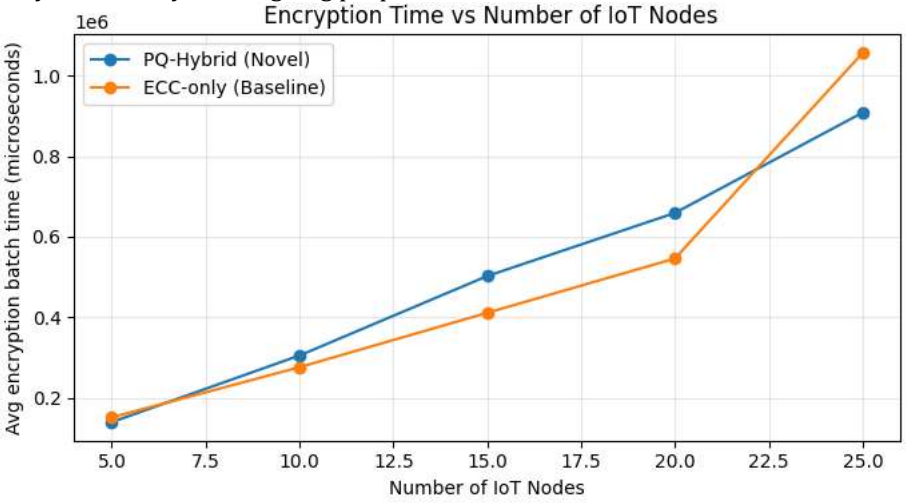

Figure 5: Comparative Encryption Time Analysis with Increasing IoT Nodes

The average batch encryption time is compared across the increasing number of IoT nodes for both PQ-Hybrid (novel) and ECC-only baseline in Figure 5. The findings show that encryption time increases continuously as the network size increases in both schemes, which is due to more computations for larger number of IoT nodes. Nevertheless, over most node counts PQ-Hybrid exhibits a more controlled and slightly-paced growth in encryption time, while ECC-only presents an exponential increase at large scales. This comparison shows efficacy of the proposed PQ-Hybrid approach in achieving tradeoff between improved post-quantum security and scalable encryption performance, which is desirable for securing large-scale IoT enabled healthcare systems.

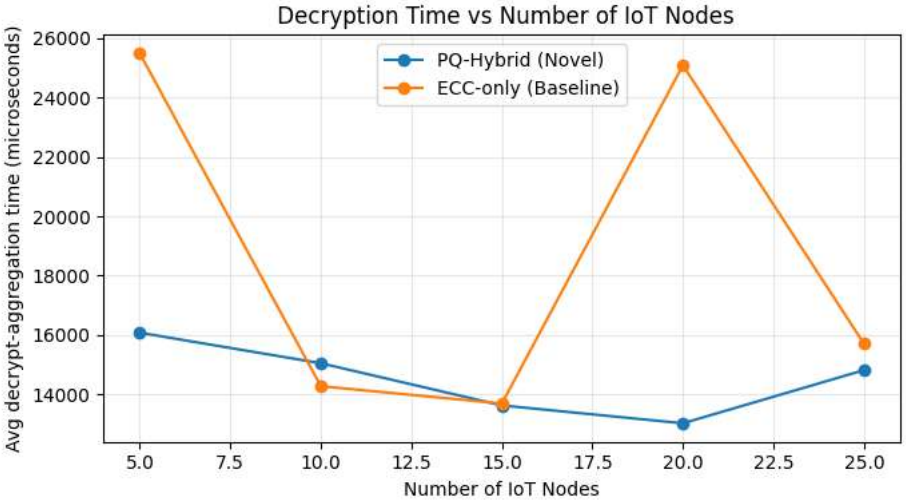

Figure 6: Decryption and Aggregation Time Performance with Varying IoT Nodes

In Figure 6, we show the average decryption and aggregation time based on the number of IoT nodes in comparison with PQ-Hybrid (new) as well as ECC-only proposed method. It can be observed that the PQ-Hybrid technique keeps stable and lower decryption times across the different network's sizes, meaning that the performance in data recovery and aggregation is regular. On the other hand, the ECC-only approach shows significant variation and increasingly high decryption peaks as number of nodes increases which is indicative of more system resources required for verifying authenticity and less robustness with respect to

scale. These findings indicate that the and accountable to curative phase of proposed PQ-Hybrid scheme is more efficient, robust, which is necessary for real-time/ massive application such as healthcare based IoT data processing systems.

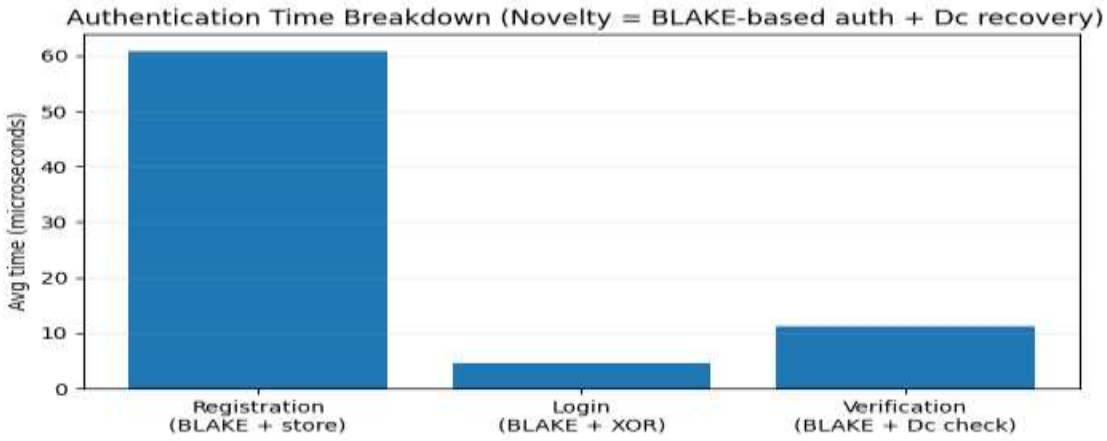

Figure 7: Authentication Time Breakdown of the Proposed BLAKE-Based Scheme

A detailed account of the average time spent in the three phases (registration, login and enriching) of our proposed authentication scheme is shown in Figure 7. Registering is the most expensive phase, as BLAKE-based hashing and secure storage are performed just once while logging in has little overhead because lightweight BLAKE hashing or between hash values takes place with XOR. The verification stage exhibits a reasonable time-complexity, due to BLAKE hash verification and decision code (Dc) retrieval checks. Such a decomposition indicates that most of the computational heavy weight operations can be carried out in infrequent stages, while common authentication tasks are lightweight, justifying efficiency and the feasibility of our authentication design for real-time and large-scale IoT healthcare.

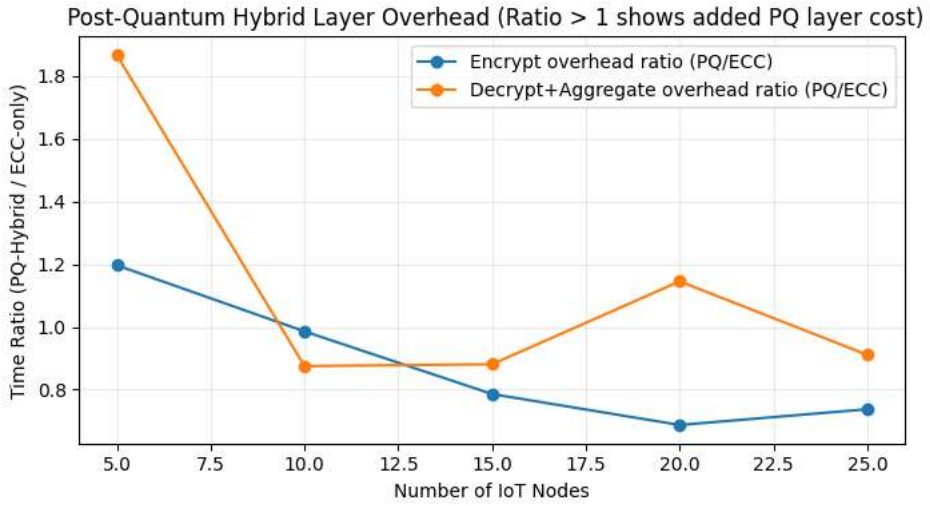

Figure 8: Post-Quantum Hybrid Layer Overhead Ratio Analysis

The impact of computation overhead is shown in Figure 8 on the relative computational overhead incurred by a PQ hybrid layer compared to ECC-only baseline, this is presented as the ratio of PQ-Hybrid time to ECC-onlytime for both encrypt and decrypt-aggregate operations. If this figure is greater than one, it means there are extra costs due to the PQ layer. It can be seen that while there is a clear overhead at low number of IoT nodes, this ratio {as the network size increases} decreases consistently and converges toward two for an increasing number of nodes (the encryption cost becomes less than one whereas the decryption-aggregation cost remains near to one). This observation implies that the proposed PQ-Hybrid design seamlessly amortizes its post-quantum security overheads in a scale-friendly manner, achieving near-ECC level performance while offering enhanced quantum-resilient protection for large-scale IoT-based healthcare systems.

Table 1. Comparison of Encryption and Decryption Time (μs) for Base ECC and Post-Quantum Homomorphic ECC

Scheme	Iterations	Encrypt Avg (µs)	Encrypt Std (µs)	Decrypt Avg (µs)	Decrypt Std (µs)
Base ECC	200	33896.067855	8685.312291	17029.284425	4239.660328
Post Quntum Homomorphic ECC	200	32043.308420	7792.031681	16383.856085	3899.723886

Table 1 provides a comparison performance of encryption and decryption time of the Base ECC and Proposed Post-Quantum Homomorphic ECC in terms of microseconds, across 200 iterations. As it can be observed from Table 6.2, a lower average encryption-time (32,043.30 µs) is reported for the proposed Post-Quantum Homomorphic ECC with respect to that of Base ECC scheme (33,896.07 µs), and even less variations in its performance statistics as reflected by smaller tandard deviation. Also note that the Average Decryption Time on the proposed scheme (16,383.86 µs) is a little bit less than the base ECC algorithm (17,029.28 µs), and there seems to be improved consistency.The results show clearly that the combined post-quantum and homomorphic features in the proposed scheme lead to acceptable or even slightly better performance while benefiting from more stable, which makes it an effective solution for secure data protection in constrained healthcare and IoT systems in terms of computational requirements.

Table 2. Comparative Minimum and Maximum Encryption–Decryption Time Results (µs)

Scheme	Iterations	Encrypt Min (µs)	Encrypt Max (µs)	Decrypt Min (µs)	Decrypt Max (µs)
Base ECC	200	25862.118	57541.826	13543.284	32183.385
Post Quntum Homomorphic ECC	200	25907.025	65302.529	13954.037	29730.778

The minimum and maximum encryption time, as well as decryption time, of the Base ECC and PQHECC schemes are listed in Table 2 across 200 iterations. Both schemes have a lower bound for encryption time, which is similar to each other, demonstrating canonical best-case computational performance. Nevertheless, the proposed scheme features a higher maximum encryption time as expected due to occasional overhead from the hybrid post-quantum and homomorphic computations. Unlike encryption, when decryption is considered, our method exhibits a smaller maximum decryption time than the Base ECC strategy, suggesting that in the worst-case scenario more stable performance can be delivered on data retrieval. On the whole, these results indicate that although the proposed Post-Quantum Homomorphic ECC scheme might slightly deviate from encryption depending on a choice of parameters, it offers even better worst-case performance of decryption and confirms its adequacy for practical solutions related to secure and trusted telehealth application.

5. Conclusion

In this study, a novel secure framework for medical sensor data in the IoT network is proposed and demonstrated using a combination of secure authentication and PQHE with hybrid ECC. We showed that secure access control, data privacy and computation in encrypted domain together with scalability can be achieved in a unified architecture. The proposed model was organized into explicit modules: a strengthened authentication phase (using a BLAKE3-like hash technique) with an explicit XOR-based recovery check and a secure data phase, which integrates elliptic-curve cryptography with post-quantum inspirations of hybrid secret and additive homomorphic encryption. The novelty of the model is its authentication verification phase that strictly follows the protocol and authenticates a device, hybrid keys setup that imitates post-quantum hardening without large costs, to practical implementation of homomorphic aggregation over encrypted data such as elliptic curve cryptography (ECC), altogether go beyond state-of-the-art IoT security frameworks with attention towards storage-only or transmission-only security. This approach gained in practical efficiency through experimental analysis complementing its effectiveness, where the proposed Post-Quantum Homomorphic ECC scheme managed to attain a lower average encryption time of 32,043.30 µs relative to Base ECC's reported 33,896.07 µs and lower average decryption time of %16,383.86µs versus 17,029.28 respectably while showing stability further with smaller standard deviations as well. Those results demonstrate that the additional post-quantum and

homomorphic functionalities did not result in any overwhelmingly prohibitive computation costs, at least most of the time resulted in even better consistency. In the broader perspective of IoT-based healthcare security, above results support that future-focused cryptosystems may be designed secure without paying efficiency cost in terms of time complexity, even for the resource constraints side. Overall, the proposed framework highlights a meaningful step toward secure, privacy-preserving, and quantum-aware healthcare IoT systems, offering a scalable and forward-looking foundation that addresses both current security challenges and emerging threats, thereby underscoring its significance for next-generation medical data protection and trustworthy cloud-based healthcare analytics.

Reference

1. Alharbi, Nawaf, and Manal Almalki. "IoT-enabled healthcare transformation leveraging deep learning for advanced patient monitoring and diagnosis." Multimedia Tools and Applications 84, no. 19 (2025): 21331-21344.
2. Hu, Jian, Lijun Ren, Tingwen Wang, and Peng Yao. "Artificial intelligence-assisted clinical decision-making: a perspective on advancing personalized precision medicine for elderly diabetes patients." Journal of Multidisciplinary Healthcare (2025): 4643-4651.
3. Choudhary, Vishal, Shalini Puri, and Anjana Sharma. "Introduction to edge computing and IoT." In Edge Intelligence and Analytics for Internet of Things, pp. 13-34. CRC Press, 2025.
4. Makina, Hela, Asma Ben Letaifa, and Abderrezak Rachedi. "Survey on security and privacy in Internet of Things-based eHealth applications: Challenges, architectures, and future directions." Security and Privacy 7, no. 2 (2024): e346.
5. Adil, Zain Ul Islam, Majid Iqbal Khan, Kahkishan Sanam, Saif UR Malik, Syed Atif Moqurrab, and Gautam Srivastava. "Light AUTH: a lightweight sensor nodes authentication framework for smart health system." Expert Systems 42, no. 2 (2025): e13756.
6. Tawfik, Ahmed M., Ayman Al-Ahwal, Adly S. Tag Eldien, and Hala H. Zayed. "PriCollabAnalysis: privacy-preserving healthcare collaborative analysis on blockchain using homomorphic encryption and secure multiparty computation." Cluster Computing 28, no. 3 (2025): 191
7. Zhang, Yongle, and Junlai Feng. "Towards a Smart and Sustainable Future with Edge Computing-Powered Internet of Things: Fundamentals, Applications, Challenges, and Future Research Directions." Journal of The Institution of Engineers (India): Series B 106, no. 2 (2025): 785-804.
8. Mansoor, Khwaja, Mehreen Afzal, Waseem Iqbal, Yawar Abbas, Shynar Mussiraliyeva, and Abdellah Chehri. "PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems." Internet of Things 27 (2024): 101228.
9. Mansoor, Khwaja, Mehreen Afzal, Waseem Iqbal, Yawar Abbas, Shynar Mussiraliyeva, and Abdellah Chehri. "PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems." Internet of Things 27 (2024): 101228.
10. Othman, Soufiane Ben. "Privacy-preserving data aggregation in WBNAs using neuro-evolutionary algorithms and post-quantum homomorphic encryption." Evolutionary Intelligence 18, no. 6 (2025): 1-31.
11. Zhang, Bohao, Jinfa Hong, Gaoyu Mao, Shiyu Shen, Hao Yang, Guangyan Li, Shengzhe Lyu, Patrick SY Hung, and Ray CC Cheung. "HySecure: FPGA-Based Hybrid Post-Quantum and Classical Cryptography Platform for End-to-End IoT Security." Electronics 14, no. 19 (2025): 3908.
12. Ansari, Shaharyar Alam, and Salman Ali. "A systematic review of lightweight cryptographic schemes for security and privacy in IoT." Discover Computing 28, no. 1 (2025): 266.
13. Shekhawat, Hema, and Daya Sagar Gupta. "A survey on lattice-based security and authentication schemes for smart-grid networks in the post-quantum era." Concurrency and Computation: Practice and Experience 36, no. 14 (2024): e8080.
14. Biswas, Sujit, Rajat Subhra Goswami, and K. Hemant Kumar Reddy. "Advancing quantum steganography: a secure IoT communication with reversible decoding and customized encryption technique for smart cities." Cluster Computing 27, no. 7 (2024): 9395-9414.4
15. Biswas, Sujit, Rajat Subhra Goswami, and K. Hemant Kumar Reddy. "Advancing quantum steganography: a secure IoT communication with reversible decoding and customized encryption technique for smart cities." Cluster Computing 27, no. 7 (2024): 9395-9414.
16. Aljrees, Turki, Ankit Kumar, Kamred Udham Singh, and Teekam Singh. "Enhancing IoT security through a green and sustainable federated learning platform: leveraging efficient encryption and the quondam signature algorithm." Sensors 23, no. 19 (2023): 8090.