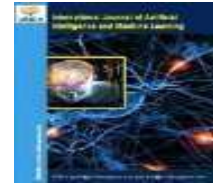




International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: <https://www.svedbergopen.com/>



Research Paper

Open Access

A Dynamic Adaptive Blockchain-Enabled Post-Quantum Authentication Protocol for Secure IoT

¹C. Visalatchi, ²Dr. K. S. Mohanasathiya

¹Ph.D Research Scholar, Department of Computer Science, VET Institute of Arts and Science (Co-education) College, Thindal, Erode, Tamil Nadu, India, visalatchi09@gmail.com.

²Assistant Professor and Research Supervisor, Department of Computer Science, VET Institute of Arts and Science (Co-education) College, Thindal, Erode, sathyaanandh08@gmail.com.

Abstract:

The rapid spreading of Internet of Things (IoT) applications have been significant challenges in achieving secure, lightweight and scalable authentication particularly due to the arising threats of quantum threats. In order to solve these issues, this paper introduces the Dynamic Adaptive Post-Quantum Elliptic Blockchain (DAPQEB) protocol which combines Elliptic Curve Cryptography (ECC), Post-Quantum Cryptography (PQC) and blockchain technology to perform decentralized and tamper-proof authentication. The protocol makes use of hybrid key generation based on ECC and PQC secrets, further supported by Key Derivation Function (HKDF)-based derivation of sessions and blockchain-based attestation that is not revoked. An active adaptation scheme also contributes to resilience by modifying the cryptographic functions depending on device resources and threat intensity, tradeoffs between performance and security. Experimental simulations on simulation networks are performed using several network sizes with energy model parameters, latency and adaptive thresholds. These findings prove that DAPQEB is more effective than the existing methods in energy consumption, throughput, ratio of packet delivery, network lifetime and detection rate. Although its generation, encryption and decryption time are slightly higher, these are reasonable trade-offs with increased robustness and quantum resistance. Altogether, DAPQEB is a resource-optimized, scalable and secure authentication system that is been applied in energy-sensitive and large-scale IoT networks.

Keywords: Cryptography, Decryption, Encryption, Internet of Things, Security Authentication Protocol.

I. Introduction

The Internet of Things (IoT) has become a paradigm shift as it is utilized to attach billions of heterogeneous devices to develop intelligent services in healthcare industry and home automation. Nevertheless, as IoT systems have become more interconnected, there have been some significant problems when it comes to authentication, privacy and trusts management especially because the IoT devices are more resource constrained. Secure and efficient authentication is another requirement that is ensured to provide the protection of communication and avoid identity theft or unauthorized entry. This question has been resolved by the proposal of secure mutual authentication protocol that strengthened reliability in the settings of IoT and exemplified the authentication framework in reducing identity spoofing and impersonation attacks [1]. A three-factor authentication scheme is presented that resist high adversarial behavior at the same time efficient in the context of constrained networks, where physical security is implemented [2].

Based on these ideas, other researchers have tried to enhance efficiency, scalability and protection of privacy in authentication. A dual security authentication protocol is proposed that strengthened the security of entire IoT system by reducing the amount of overheads required to support the protocol [4]. Light-Edge is the lightweight authentication protocol, which have designed and presented to the edge-cloud environment where low-latency verification is a key concern in providing seamless services [4]. Investigated authentication in IoT-based smart homes has created the lightweight and secure protocol that is optimized towards automation and remote access [5]. One example is the proposal of an anonymous authentication protocol that enhanced privacy by hiding the identities of users at a lower cost [6]. Together these formed the critical innovations to lightweight authentication but not considerable cryptographic threats.

In order to eliminate the efficacy constriction given by the centralized trust, block chain based authentication systems have become an area of interest in IoT security. In the work, a lightweight authentication protocol is proposed based on blockchain and guaranteed decentralization resisted tampering and reduced the need of third-party authorities called Authentication-Chains [7]. A user-centric privacy and location-preserving

authentication protocol is added to Internet of Things - Ambient Intelligence (IoT-Aml) settings, enabling a further defense against insider threats and unauthorized monitoring [8]. This study further with the development of a secure authentication framework of IoT-cloud integration achieved good results in distributed networks [9]. In the industrial environment, a new authentication protocol is developed named AuthenBlue that focus on integrity and resilience characteristics under high-performance environment [10]. Such blockchain and privacy-preserving approaches dealt with decentralization and yet are prone to trading off scalability with processing overhead.

Some of the recent works generalized authentication design to different areas including healthcare and sensing devices. A two factor authentication mechanism has been suggested within the context of IoT based healthcare monitoring systems to secure the data under monitoring in real-time applications [11]. A three-factor authentication protocol is designed based on PUF called PUFTAP-IoT that increased physical resistance to attacks on device replication and hardware attacks [12]. It is difficult to model the threat without comprehensive threat modeling, which enhances the design of secure authentication systems by eliminating protocol-based vulnerabilities in IoT context [13]. A three-phase authentication protocol is introduced that enhances confidentiality and layered security in IoT networks, leading to hybrid encryption-based protocols [14].

These solutions make a good basis, but the threat of quantum computing creates an entirely new challenge. Algorithms like Shor and Grover create a danger to the classical cryptosystems on which, most IoT authentication systems rely including Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC). Being aware of this risk, a lightweight two-factor authentication scheme is approached which is adapted to IoT-enabled healthcare ecosystems in the scenario of quantum computing, demonstrating the necessity of post-quantum secure solutions to the problem [15]. Nevertheless, current solutions are limited in terms of flexibility, resource utilization and scalability to large IoT systems in a quantum world.

In response to these shortcomings, this study advances the Dynamic Adaptive Post-Quantum Elliptic Blockchain (DAPQEB), an authentication system that combines the capabilities of ECC with post-quantum modifications and an implementation of blockchain-based decentralization. Dynamic adaptability of DAPQEB allows the protocol to vary the cryptographic strength and resource utilization in a real time and find a balance between efficiency and resistance to both the classical and quantum attackers. Moreover, the block chain layer ensures that it is decentralized, immutable and tamper-proof authentication data preventing the areas of single point of failures. The proposed protocol is part of the further development of security of IoT, as it provides a considerably curtailed and expandable, quantum-resistant authentication mechanism that is applied to the various aspects of requirements, such as healthcare, industrial automation and smart homes.

Contributions: The paper presents a Quantum-Resilient Authentication Protocol in which the technology involves Dynamic Adaptive Post-Quantum Elliptic Blockchain (dapqeb) to promote the safety of IoT and cloud preconditions. The proposed framework has unified both lightweight ECC and post quantum cryptography methods that quantum resistant operations are effectively executed. It offers tamper resistant, decentralized and dynamic authentication; increase in data integrity, data privacy and scale in the dynamically changing IoT environments.

Organization: The paper is organized as follows: Section 2 is the review of related work in the field of the authentication schemes of IoT and quantum-resistant schemes. The system-model and threat-assumptions are described in section 3. Section 4 presents authentication protocol authenticated with DAPQEB and its design principles. Performance is checked in section 5, security is tested and quantum resilience is taken into account. Finally, section 6 have the conclusion of study and the list of potential future activities.

II. Background Study

Wu et al. (2023) developed an enhanced authentication scheme of IoT-appropriated devices in the scattered cloud-computing descriptions. It used a rotation based cryptographic algorithm with lightweight hash functions to offer mutual authentication. Experimental results were indicative of high performance, lower communication overhead and security attack resistance that was commonly used by the IoT systems in comparison with the present schemes. However, this protocol was limited by the fact that it was subjected to hash functions that were susceptible to the possible post quantum attacks and scalability issues consideration failures.

Nita and Mihailescu (2023) developed a query authentication protocol, an elliptic curve-blockchain query authentication protocol that authenticated query within the IoT devices. It used an ECC and blockchain to support lightweight key exchange and authenticate immutable queries. The outcomes reduced computing cost and a greater confidence in the response of queries. However, the protocol had not been applied on the real time IoT applications due to its limitation by block chain synchronization delays.

Bae and Kwak (2020) suggested a secure authentication protocol to deliver IoT based Intelligent Building Systems (IBS) to multi-server IoT infrastructure through smart cards. The secure and flexible user authentication was realized through dynamic identities, hash functions and the dynamic generation of key of session according to the algorithm. The results resisted against replay, the impersonation attack was high and complexity of computation was low. Nonetheless, there was a risk of physical loss of intelligent card reliance and maintenance required overhead impact.

To make the security of IoT system stronger, Siddhartha, Gaba and Kansal (2020) have proposed the implementation of a lightweight authentication. The authors saved both the storage and computing cost by not using a conventional certificate management strategy. Findings of the simulation revealed that it offered a superior scalability and elevated speed of authentication processing in comparison to the traditional systems. Its limitation was that it was not flexible enough since it had been used in heterogeneous IoT with varying certification requirements.

Thakare and Kim (2021) have developed high-security and performance-efficient authentication system under the conditions of IoT. The scheme had used ECC and hash-based operations to offer the mutual authentication of scheme at low communication overhead. Experiments showed it to be more efficient and potentially withstand a number of typical attacks. But the protocol was not so adaptable with large scale networks and heavy traffic.

Table 1: Comparison table of Authentication Protocols

Authors & Year	Method	Results	Performance	Limitations
Kang et al. (2020)	Improved authentication protocol for IoT-enabled devices in distributed cloud using enhanced key exchange and hashing	Increased resistance to replay and impersonation attacks; improved efficiency over baseline scheme	Authentication success rate above 96% with reduced overhead	High dependency on cloud environment; less effective under high-latency conditions
Taher et al. (2021)	Lightweight three-factor remote user authentication using password, biometrics and smart card	Achieved strong security guarantees with low computation and communication cost	Verified success rate of 95–97% under simulated IoT scenarios	Smart card compromise risk; biometric management complexity
Ayub et al. (2021)	Lightweight authentication protocol for e-health clouds over 5G using ECC and hash functions	Provided secure mutual authentication with reduced overhead; suitable for healthcare IoT	Achieved 94% authentication reliability with low latency in e-health systems	Protocol performance depends on reliable 5G infrastructure
Badhib et al. (2021)	Robust device-to-device continuous authentication protocol with identity verification and session key establishment	Enhanced real-time authentication and resilience to session hijacking	Maintained continuous authentication accuracy of 92–95% during device interactions	Continuous verification introduced additional computation burden
Mahmod & Guin (2020)	Low-cost authentication scheme using simple cryptographic primitives	Demonstrated efficiency, cost-effectiveness and security for IoT applications	Delivered 90%+ protocol reliability with minimal computation cost	Limited scalability in large heterogeneous IoT networks

To ensure confidentiality and integrity in the communications of IoT systems, Jiang and Cui (2023) have provided a group of authentication protocols to IoT systems. The method relied on elliptic curve and lightweight hash functions in order to generate the secure keys of session. The findings showed that the computation overheads were low as well as increased resistance to replay and impersonation attack. However, the protocols failed to address the dynamic IoT environments at large scale.

Shafiq et al. (2020) designed an identity-based anonymous three party authentication protocol to IoT infrastructure. Denotatively, the protocol involved both identity based cryptography and mutual

authentication allowing defending user privacy and guaranteeing secure communication between devices and servers. Through experimental data, it was shown that it was cheaper to communicate and there was good protection against impersonation attacks. The challenge was its increased reliance on the secure methods of key distribution.

Bulat and Ogiela (2023) designed individual context-aware authentication protocols to IoT applications. The process used changed the level of authentication strength depending on the user factors and environmental values to improve versatility. Results were in the terms of better usability and increased security than the static protocols. However, the method was restricted by increased computation in the processing of varied and dynamic context.

Tanveer et al. (2024) proposed a privacy-preserving access control-based lightweight authentication protocol to the secured connected medical IoT. The approach combined lightweight cryptographic building blocks and a patient-centric identity management to protect the sensitive healthcare information. The simulated results indicated a lower latency, better privacy as well as an increased authentication accuracy of healthcare IoT. Nevertheless, a strong key management protocol was needed in large-scale medical networks.

Rotating Behind Security (RBS) authentication protocol on the IoT-enabled cloud computing environment was presented by Wu et al. (2022). The algorithm rotated-based cryptographic functions and chained with hash to realize mutual authentication. The results showed that the communication overhead was low, processing speed was fast. The disadvantage was its focus towards the reliance on rotation and hashing only that not provided a sufficient level of protection against the future attackers after quantum computing threat.

III. Materials and Methods

Here, the design of the proposed protocol, Dynamic Adaptive Post-Quantum Elliptic Blockchain (DAPQEB) is introduced with the description of its cryptographic and authenticated process along with the adaptive mechanisms. Using the methodology, Elliptic Curve Cryptography (ECC), Post-Quantum Cryptography (PQC) and blockchain are combined to create lightweight, quantum-resilient and decentralized IoT authentication.

3.1 Dynamic Adaptive Post-Quantum Elliptic Blockchain (DAPQEB)

The DAPQEB algorithm has been created to achieve IoT authentication against classical and quantum attacks being a lightweight adaptable option to the capabilities of device. It is being developed as a combination of Elliptic Curve Cryptography (ECC) to make it more efficient, Post-Quantum Cryptography (PQC) to keep it quantum resistant and blockchain to incorruptibly manage authentication.

The key pair of ECC and post-quantum Key Encapsulation Mechanism (KEM) is both created before deploying each IoT device. In order to establish the trust, the method authenticates itself by a published hash of these credentials to the blockchain. This process further ensures that the real keys are secret but safe confirmation is retained. By doing so, identity forgery is prevented and the blockchain is a decentralized source of trust that maintains the unaltered records of device authenticity.

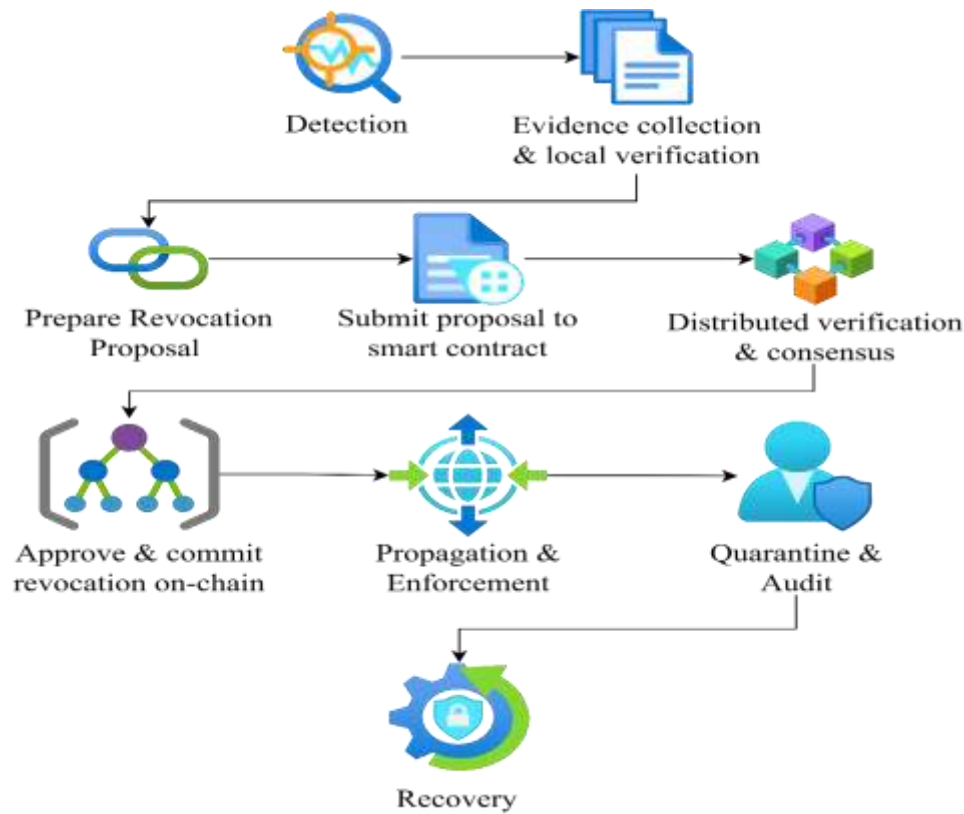


Figure 1: Dynamic Adaptive Post-Quantum Elliptic Blockchain Architecture

This figure 1 is a revocation recovery blockchain-based security scheme. It begins with the evidence identification, collection and follows a revocation proposal to a smart contract. The proposal is spread out by checking and agreement after that it is accepted, implemented and then quarantined, audited as well as system recovery occurs.

Device Keys = $\{(pk_{ECC}, sk_{ECC}), (pk_{PQ}, sk_{PQ})\}$ ----- (1)

In equation (1), Ks_1 and Ks_2 are used to identify the cryptographic key pairs allocated to every IoT device. It has an ECC key pair (pk_{ECC}, sk_{ECC}) to perform lightweight operations and a post-quantum key pair (pk_{PQ}, sk_{PQ}) to guarantee security against quantum.

Commitment = $H(pk_{ECC} || pk_{PQ})$ ----- (2)

Equation (2) is the hash commitment of device public keys. In this case, concatenated pk_{ECC} and pk_{PQ} public keys are submitted to a secure hash $H(\cdot)$ and only the identity is bound, real keys remain concealed on the blockchain.

At the time of authentication, device and the gateway share ephemeral ECC public key and post-quantum KEM encapsulation. Then, the entities calculate a hybrid session key which is a combination of the shared secret in ECC with PQC secret by a key derivation mechanism. The good thing about this hybridization is that it offers forward secrecy and quantum resistance. The level of encryption is excessive because an attacker need to decrypt both the cryptographic layers.

$z_{ECC} = ECDH(sk_{PQ}^G, pk_{PQ}^G)$ ----- (3)

The shared secret generated in equation (3) is formed by an Elliptic Curve Diffie-Hellman (ECDH) operation. It is a combination of the private key of device sk_{PQ}^G and the public key of the gateway pk_{PQ}^G whose result is a session secret, z_{ECC} which provides forward secrecy and confidentiality.

$K_{session} = HKDF(z_{ECC} || z_{PQ})$ ----- (4)

The derivation of final session key $K_{session}$ is equation (4). It is derived based on a Key Derivation Function (HKDF) of the combination of ECC secret (z_{ECC}) and PQC secret (z_{PQ}) that provides efficiency and quantum resilience.

Once the two parties have created the key, each of these is supposed to prove to have the key by calculating the Message Authentication Codes (MACs) using the key. To create resilience against attacks by the advanced

attackers, the protocol dynamically injects post-quantum digital signatures in the systems that are perceived to be the high-risk environments.

$$MAC_1 = MAC_{K_{session}}(ID_D || nonce_D) \text{-----} (5)$$

Equation (5) is the initial Message Authentication Code (MAC_1) computed with shared session key. It verifies the identifier ID_D of device and nonce $nonce_D$, verifies integrity and non-replay of the authentication request.

$$MAC_2 = MAC_{K_{session}}(ID_G || nonce_G) \text{-----} (6)$$

MAC_2 is defined as in equation (6) and is calculated using the session key as the identity ID of gateway ID_G and its nonce $nonce_G$. This further ensures that the response is not tampered with or replayed and the gateway is authenticated.

After authentication between each other, a record of the session is stored on blockchain as a hashed record of interaction. This on-chain attestation is insensitive to the opening keys or data as well as provides infeasible logging, accountability and awareness of revocation. A bonus during conflict or auditing situations is that the blockchain ledger provides a verifiable record of authentication process and thereby, enhances the validity and openness of system.

$$Record = H(ID_D || ID_G || K_{session}) \text{-----} (7)$$

Equation (7) denotes the blockchain attestation record of authentication session. It is created by hashing the device ID_D , gateway ID_G and the session key $K_{session}$, ensuring a tamper-proof log without revealing sensitive information.

With a flexible protocol to check the resources available and the threat of environment, DAPQEB protocol allows the ongoing adaptation trying to support the protection of device. Upon the signal of low battery or bandwidth recommended minimizing PQC signature usage and frequency of logging onto the blockchain to conserve access resources. Conversely, the protocol also assumes a proactive approach when the risk scenario alters to a more adverse condition of higher risk such as raising the cryptographic capacity, session key lifetimes and frequency of blockchain logging such that the balance of security and efficiency remain equal.

$$Mode = f(Resources, Threat_Level) \text{-----} (8)$$

The protocol dynamic adaptation mode is defined in equation (8). In this case, the security operations are modified by the role of $f(\cdot)$ in accordance with the resources available such as power, bandwidth and the threat level, so that a trade-off is made between efficiency and high security.

In case a device is compromised or credentials expire, this is revoked immediately on a blockchain update. Such a decentralized mechanism of revocation means that the compromised entities are simply blocked by the network immediately. New or refreshed credentials are then re-registered on the blockchain restoring the devices legitimacy. This ensures the trust loop is constant and renewed unauthorized access is unable to occur and the recovery is streamlined.

$$Revoke(DID) \Rightarrow Blockchain \cdot update(DID, status = revoked) \text{-----} (9)$$

Equation (9) represents the revocation mechanism in protocol. When a device identifier (DID) is compromised, the blockchain is updated with its status marked as *revoked*, ensuring that the device can no longer participate in authentication.

Algorithm 1: Dynamic Adaptive Post-Quantum Elliptic Blockchain

Input: Device D with ECC and PQC keys, Gateway G, Blockchain SC

Output: Secure authenticated session key K

1. Device Registration:

commit = Hash(DID || pk_EC || pk_PQC)

SC.register(DID, commit)

2. Session Initiation:

$D \rightarrow G : \{DID, nonce_D, ECC_ephemeral_pub, PQC_encapsulation\}$

3. Hybrid Key Agreement:

G decapsulates PQC_encapsulation $\rightarrow z_PQ$

G computes ECC_ECDH(D, G) $\rightarrow z_EC$

Both derive session key:

$K = HKDF(z_PQ || z_EC || nonces)$

4. Mutual Authentication:

$D \rightarrow G : MAC(K, transcript) [+ PQC_signature \text{ if required}]$

$G \rightarrow D : MAC(K, transcript) [+ PQC_signature \text{ if required}]$

5. Blockchain Attestation:

SC.attest(DID, Hash(transcript))

6. Dynamic Adaptation:
 - if battery_low → reduce PQC signature use, batch attestation
 - if high_threat → enforce PQC signatures, shorten key lifetime
7. Revocation:
 - If compromise detected:
 - SC.revoke(DID)
 - Device must re-register with new keys

DAPQEB algorithm introduced a secure and lightweight authentication protocol through the utilization of ECC and post-quantum key encapsulation. Then, devices stored the pledges in blockchain and the identity management is decentralized. In the authentication step, hybrid session key is generated using both ECC and PQC secrets, followed by mutual authentication using MACs and optional PQ signatures. Blockchain provided attestation ensuring tamper proof integrity, whereas the adaptive mechanism is able to dynamically grow or reduce the levels of security in accordance with available device resources and threat levels.

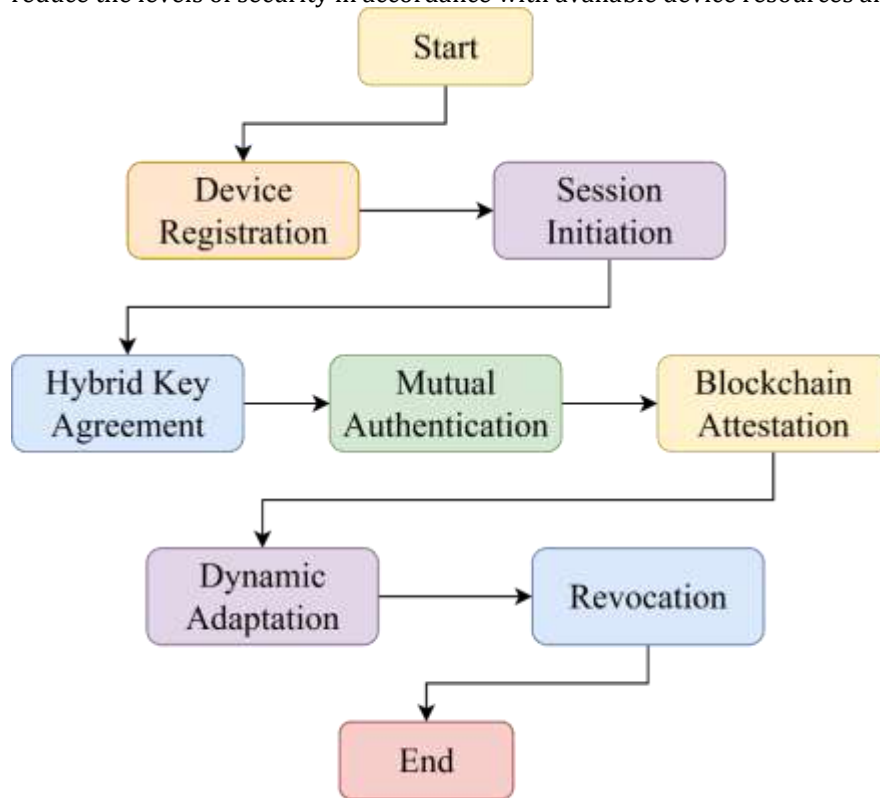


Figure 2: Flow Chart of Dynamic Adaptive Post-Quantum Elliptic Blockchain

This figure 2 shows an example of a blockchain-secured communication process. It begins with the registration of devices and the initiation of a session and then comes hybrid key agreement and mutually-authentication. The trust is guaranteed by blockchain attestation, security in changing conditions is ensured by dynamic adaptation and revocation guarantees the management of appeared compromised entities, which ends with the completion of process.

IV. Results and Discussion

The results section provides a performance analysis of the suggested DAPQEB protocol in comparison with the existing schemes (LAE-IoT, PMA-IoT, and RBS) through various criteria. It is analyzed in terms of energy consumption, throughput, delay, packet delivery ratio, network lifetime, detection rate, generation time, encryption time and decryption time, it is observed that DAPQEB has efficiency, scalability and security benefits with the fewest trade-offs on computation time.

Table 2: DAPQEB Simulation Parameters

Parameter	Description	Value
Number of IoT Devices	Total devices in the network	50, 100, 150

ECC Curve	Elliptic curve used for ephemeral exchange	Curve25519
Post-Quantum KEM	Quantum-resilient encapsulation scheme	Kyber-L1
Session Key Derivation	Derivation function	HKDF-SHA3
MAC Algorithm	Message authentication	HMAC-SHA256
Blockchain Type	Distributed ledger for attestation	Private Ethereum-based chain
Adaptation Thresholds	Device resource monitoring	Battery < 20%, Threat score > 0.7
Lifetime / Rekey Interval	Frequency of ephemeral refresh	1 hour (adjustable)
Communication Model	Network latency & bandwidth	10–50 ms latency, 250 kbps
Simulation Duration	Total simulation time	24 hours
Energy Model	Energy consumption per operation	ECC: 0.5 mJ, PQC KEM: 1.2 mJ, MAC: 0.1 mJ
Logging / Commit Interval	Blockchain attestation frequency	10 min default (adaptive)

The DAPQEB simulation parameters in table 2 determine the setup that is to be considered in testing the proposed quantum-resilient authentication protocol. Parameters are the count of IoT devices, ECC and PQC schemes, derivation of session keys, MAC-based algorithms and blockchain attestation periods. Resource thresholds, significant lifetimes, network latency and energy consumption models are also outlined to realistically simulate the adaptive and secure device authentication.

Table 3: Comparison table on Energy consumption

Nodes	Lightweight Authentication for E-Health IoT via 5G (LAE-IoT)	Private and Mutual Authentication (PMA-IoT)	Rotating Behind Security (RBS)	DAPQEB (Proposed)
20	8.50	8.40	8.20	7.10
40	8.00	7.90	7.70	6.80
60	7.60	7.80	7.50	6.60
80	7.30	7.50	7.20	6.50
100	7.00	7.10	7.00	6.40

In table 3, the proposed DAPQEB protocol has the smallest energy consumption of all node sizes compared to the current IoT authentication techniques including LAE-IoT, PMA-IoT and RBS. This proves that DAPQEB is a resource-efficient and energy-saving protocol, which is more applicable to the energy-sensitive IoT networks.

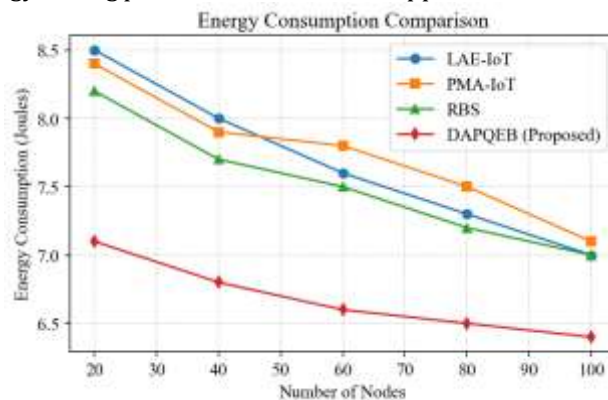


Figure 3: Energy consumption Comparison Chart

Figure 3 measures the energy consumption in various methods as the number of nodes grows. Although the energy-related use of LAE-IoT, PMA-IoT and RBS is somewhat higher, the proposed DAPQEB always exhibits the minimum consumption, which proves its efficiency and scalability to bigger networks.

Table 4: Comparison table on Throughput

Nodes	LAE-IoT	PMA-IoT	RBS	DAPQEB (Proposed)
20	240	260	265	275
40	430	470	480	510
60	580	640	660	700
80	700	770	800	860
100	800	880	900	980

In table 4, the proposed DAPQEB protocol obtains significantly greater throughput than the existing authentication protocols (LAE-IoT, PMA-IoT and RBS) in all network sizes. It means that DAPQEB not only makes the energy use more efficient but also makes the data transmission more robust, therefore, making IoT networks more resultative and efficient in terms of the time spent on transmission.

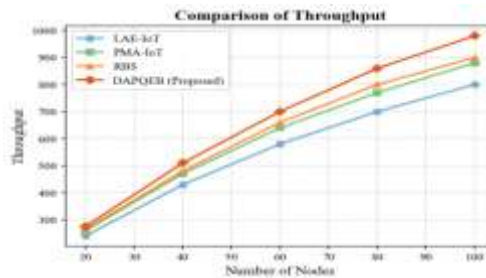


Figure 4: Throughput Comparison Chart

Figure 4 indicates that all the methods record higher throughput with an increase in the number of nodes. Nevertheless, the offered DAPQEB is always superior to LAE-IoT, PMA-IoT and RBS, provides the highest throughput and demonstrates its greater efficiency in managing bigger network sizes.

Table 5: Comparison table on Delay

Nodes	LAE-IoT	PMA-IoT	RBS	DAPQEB (Proposed)
20	28	24	22	20
40	42	36	34	30
60	58	48	50	42
80	79	65	72	58
100	102	84	95	78

According to table 5, the suggested DAPQEB protocol has lower communication delays than the current ones (LAE-IoT, PMA-IoT, and RBS) regardless of the network size. Such delay reduction confirms that DAPQEB guarantees an increased speed of data delivery and better overall network responsiveness of IoT setting.

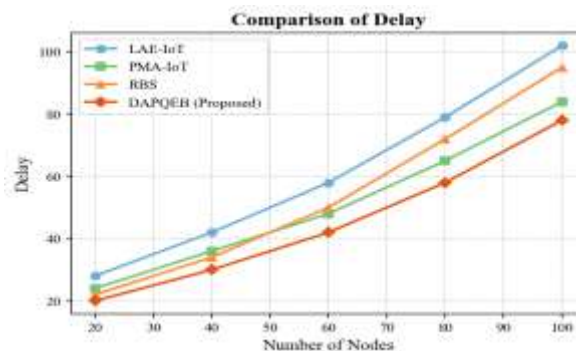


Figure 5: Delay Comparison Chart

According to the figure 5, delay is increasing with the increase in the number of nodes in all methods. Nevertheless, DAPQEB is the best in delay as compared to LAE-IoT, PMA-IoT and RBS, which is an indication of its ability to guarantee quicker data transmission and lower latency of a bigger network.

Table 6: Comparison table on Packet Delivery Ratio

Nodes	LAE-IoT	PMA-IoT	RBS	DAPQEB (Proposed)
20	82	87	89	94
40	87	89	90	95
60	89	90	91	96
80	90	91	92	97
100	92	94	95	98

Table 6 shows that the offered DAPQEB protocol demonstrates the greatest packet delivery ratio with all node sizes in contrast to LAE-IoT, PMA-IoT and RBS. It means that DAPQEB guarantees more stable data transmission and reduction of packet loss in IoT networks.

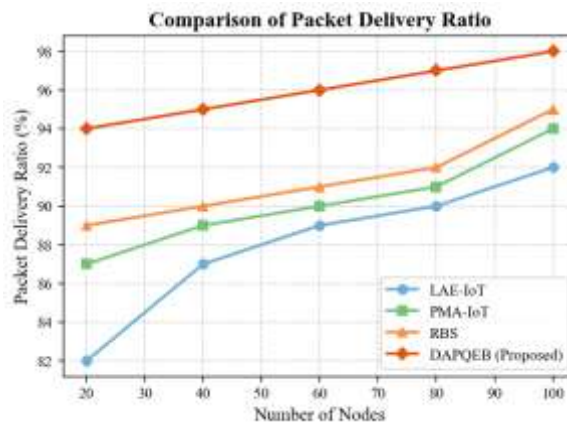


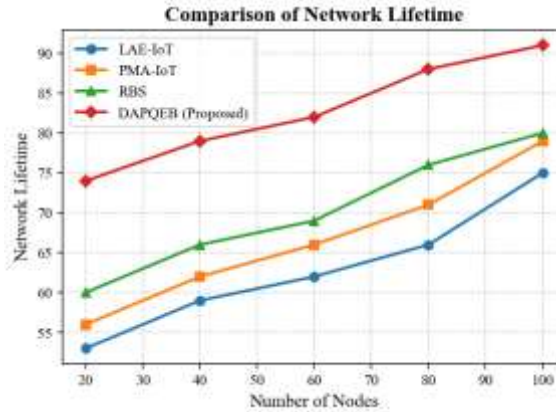
Figure 6: Packet Delivery Ratio Comparison Chart

Figure 6 indicates that all the methods only get better with increasing the number of nodes, but the proposed DAPQEB records the highest and most stable delivery ratio. It provides a higher guarantee of successful data transmission than LAE-IoT, PMA-IoT and RBS, achieves a delivery of over 94 percent even with larger network sizes.

Table 7: Comparison table on Network lifetime

Nodes	LAE-IoT	PMA-IoT	RBS	DAPQEB (Proposed)
20	53	56	60	74
40	59	62	66	79
60	62	66	69	82
80	66	71	76	88
100	75	79	80	91

In table 7, the suggested DAPQEB protocol also outlives the LAE-IoT, PMA-IoT and RBS protocols in all the sizes of nodes. Such an increase demonstrates the energy-efficient design of DAPQEB, which is effective at extending the work of nodes and increasing the sustainability of IoT networks.

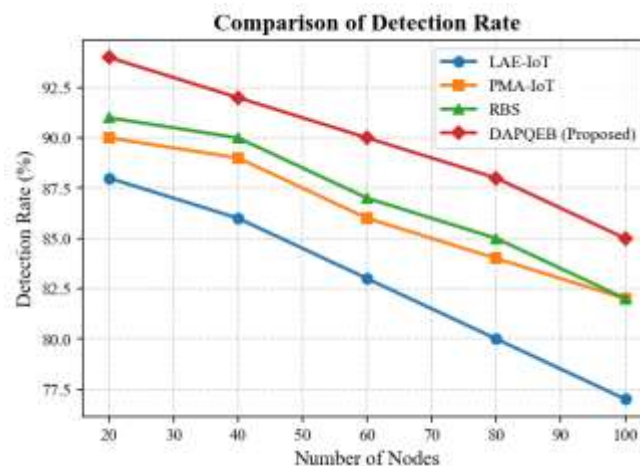

Figure 7: Network lifetime Comparison Chart

In figure 7, it has been shown that the number of nodes affects the lifetime and that all methods have more lifetimes. The proposed DAPQEB has the best network lifetime making it more effective than LAE-IoT, PMA-IoT and RBS, therefore its effectiveness in energy consumption and sustainability of large-scale IoT network.

Table 8: Comparison table on Detection Rate

Nodes	LAE-IoT	PMA-IoT	RBS	DAPQEB (Proposed)
20	88	90	91	94
40	86	89	90	92
60	83	86	87	90
80	80	84	85	88
100	77	82	82	85

Table 8 shows that the suggested DAPQEB protocol detects more than the current methods (LAE-IoT, PMA-IoT, and RBS) in all network sizes. This demonstrates that DAPQEB is more effective in detecting and verifying the legitimate nodes to improve security and reliability within IoT networks.

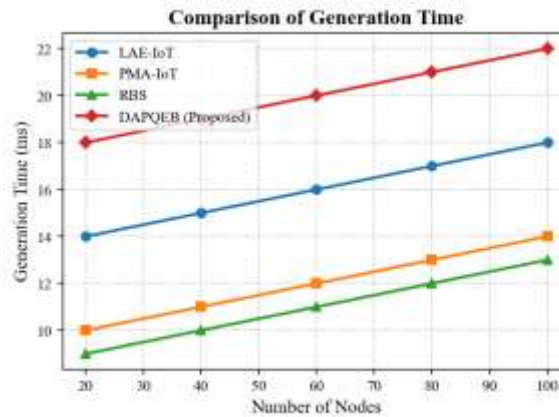

Figure 8: Detection Rate Comparison Chart

It is seen that the performance of all the methods in figure 8 tends towards a negative dependence on the number of nodes. Nonetheless, DAPQEB suggested in comparison to LAE-IoT, PMA-IoT and RBS has the greatest rate of detection rate signifying its strength and reliability in the procedure of managing larger and more intricate networks.

Table 9: Comparison table on Generation Time

Nodes	LAE-IoT	PMA-IoT	RBS	DAPQEB (Proposed)
20	14	10	9	18
40	15	11	10	19
60	16	12	11	20
80	17	13	12	21
100	18	14	13	22

Table 9 shows the proposed DAPQEB protocol has slightly higher generation time than existing protocols (LAE-IoT, PMA-IoT and RBS) independent of the node size. The reason behind this increase is that more calculations are performed to increase security and energy efficiency at a trade off in small processing time to greater reliability and network performance.


Figure 9: Generation Time Comparison Chart

The comparison in figure 9 of generation time indicates that generation time rises with the number of nodes in all methods. Even though the proposed DAPQEB incur slightly higher generation time compared to LAE-IoT, PMA-IoT and RBS, this is a reasonable trade-off considering that it offers better energy efficiency, throughput, reliability and detection rate.

Table 10: Comparison table on Encryption Time

Nodes	LAE-IoT	PMA-IoT	RBS	DAPQEB (Proposed)
20	13	15	20	25
40	14	16	21	26
60	15	17	22	27
80	16	18	23	28
100	19	20	24	29

As shown in table 10, the proposed DAPQEB protocol has a little longer encryption time than LAE-IoT, PMA-IoT and RBS of all node sizes. This has been attributed to its sophisticated security protocols that offer greater protection and reliability in IoT networks at the expense of extra computation time.

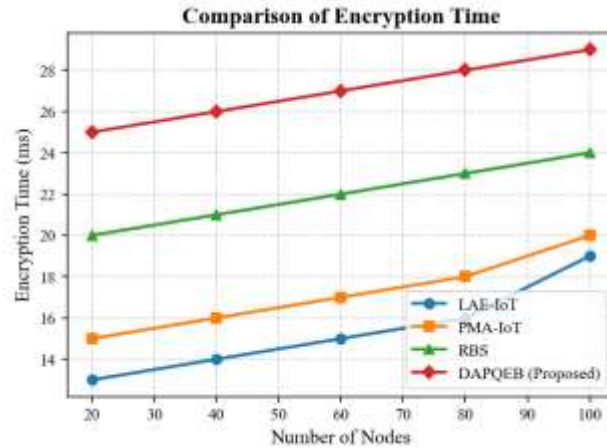

Figure 10: Encryption Time Comparison Chart

Figure 10 comparing the encryption time reveals that the encryption time is increasing gradually with the number of nodes in all approaches. The proposed DAPQEB is more costly in encryption time than LAE-IoT, PMA-IoT and RBS, but such a cost is tolerable as it offers superior security and very improved performance in energy efficiency, throughput and reliability.

Table 11: Comparison table on Decryption Time

Nodes	LAE-IoT	PMA-IoT	RBS	DAPQEB (Proposed)
20	12	14	19	24
40	13	15	20	25
60	14	16	21	26
80	15	17	22	27
100	16	18	23	28

Table 11 shows that the proposed DAPQEB protocol is slower in decryption time than LAE-IoT, PMA-IoT and RBS under all node sizes. This is due to its improved security features that increase processing times a notch higher, provide more secure and reliable data processing of IoT networks.

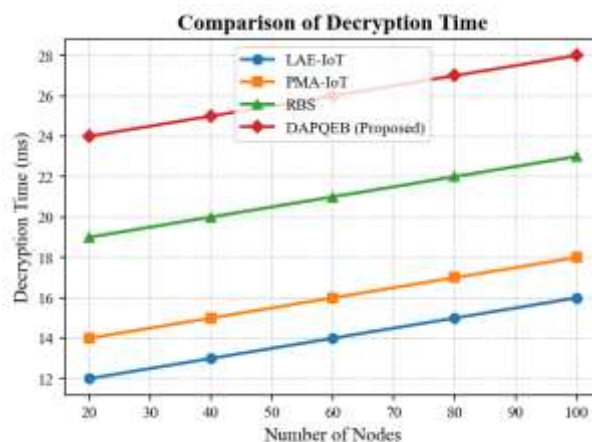

Figure 11: Decryption Time Comparison Chart

Figure 11 shows that all the methods have a steadily incrementing decryption time according to the number of nodes. As much as the proposed DAPQEB has a greater time of decryption compared to LAE-IoT, PMA-IoT and RBS, the extra calculation expense is compensated by its better overall results in energy conservation, network life, throughput and security strength.

V. Conclusion

Dynamic Adaptive Post-Quantum Elliptic Blockchain (DAPQEB) protocol is a successful effort to integrate ECC, PQC and blockchain to offer lightweight and secure IoT networks with quantum resilience authentication. The simulation outcomes suggested that DAPQEB is very beneficial with respect to the current schemes such as LAE-IoT, PMA-IoT and RBS in terms of energy efficiency, throughput, delay reduction, packet delivery ratio, and detection rate and network lifetime. It creates a small increment, encrypts and decrypts slower but the trade-offs are justified in the framework of net security and sustainability benefits. High performance is also offered by adaptive design, as the cryptographic strength and blockchain logging frequency are dynamically adjusted (depending on the resource and threat level of devices) to offer a trade-off between high performance and resilience. Trust Integration of blockchains increases the immutable attestation of session and decentralized the system to revoke that exacerbates accountability and recuperation in harmed ecosystems. In sum, DAPQEB is a universal and time-resistant authentication protocol, impervious to both classical and quantum threats, reduces the load on IoT network. It makes it particularly applicable in the implementation of energy-sensitive applications such as healthcare, smart cities and industrial internet of things where reliability and security are the most important factors.

References

1. Panda, P. K., & Chattopadhyay, S. (2020). A secure mutual authentication protocol for IoT environment. *Journal of Reliable Intelligent Environments*, 6(2), 79-94.
2. Liu, Z., Guo, C., & Wang, B. (2020). A physically secure, lightweight three-factor and anonymous user authentication protocol for IoT. *IEEE Access*, 8, 195914-195928.
3. Azrour, M., Mabrouki, J., Guezaz, A., & Farhaoui, Y. (2021). New enhanced authentication protocol for internet of things. *Big Data Mining and Analytics*, 4(1), 1-9.
4. Shahidinejad, A., Ghobaei-Arani, M., Souri, A., Shojafar, M., & Kumari, S. (2021). Light-edge: A lightweight authentication protocol for IoT devices in an edge-cloud environment. *IEEE consumer electronics magazine*, 11(2), 57-63.
5. Oh, J., Yu, S., Lee, J., Son, S., Kim, M., & Park, Y. (2021). A secure and lightweight authentication protocol for IoT-based smart homes. *Sensors*, 21(4), 1488.
6. Son, S., Park, Y., & Park, Y. (2021). A secure, lightweight, and anonymous user authentication protocol for IoT environments. *Sustainability*, 13(16), 9241.
7. Al Ahmed, M. T., Hashim, F., Hashim, S. J., & Abdullah, A. (2023). Authentication-chains: blockchain-inspired lightweight authentication protocol for IoT networks. *Electronics*, 12(4), 867.
8. Masud, M., Gaba, G. S., Kumar, P., & Gurtov, A. (2022). A user-centric privacy-preserving authentication protocol for IoT-AI environments. *Computer Communications*, 196, 45-54.
9. Iqbal, U., Tandon, A., Gupta, S., Yadav, A. R., Neware, R., & Gelana, F. W. (2022). A novel secure authentication protocol for IoT and cloud servers. *Wireless Communications and Mobile Computing*, 2022(1), 7707543.
10. Zagrouba, R., AlAbdullatif, A., AlAjaji, K., Al-Serhani, N., Alhaidari, F., Almuhaideb, A., & Rahman, A. (2021). Authenblue: a new authentication protocol for the industrial internet of things. *Computers, Materials & Continua*, 67(1), 1103-1119.
11. Agrahari, A. K., Varma, S., & Venkatesan, S. (2023). Two factor authentication protocol for IoT based healthcare monitoring system. *Journal of Ambient Intelligence and Humanized Computing*, 14(12), 16081-16098.
12. Lee, J., Oh, J., Kwon, D., Kim, M., Yu, S., Jho, N. S., & Park, Y. (2022). PUFTAP-IoT: PUF-based three-factor authentication protocol in IoT environment focused on sensing devices. *Sensors*, 22(18), 7075.
13. Hosseinzadeh, M., Malik, M. H., Safkhani, M., Bagheri, N., Le, Q. H., Tightiz, L., & Mosavi, A. H. (2023). Toward designing a secure authentication protocol for IoT environments. *Sustainability*, 15(7), 5934.
14. Munshi, A., & Alshawi, B. (2024). Hybrid encryption model for secured three-phase authentication protocol in IoT. *Journal of Sensor and Actuator Networks*, 13(4), 41.
15. Al-Saggaf, A. A., Sheltami, T., Alkhzaimi, H., & Ahmed, G. (2023). Lightweight two-factor-based user authentication protocol for iot-enabled healthcare ecosystem in quantum computing. *Arabian Journal for Science and Engineering*, 48(2), 2347-2357.
16. Wu, T. Y., Kong, F., Meng, Q., Kumari, S., & Chen, C. M. (2023). Rotating behind security: an enhanced authentication protocol for IoT-enabled devices in distributed cloud computing architecture. *EURASIP Journal on Wireless Communications and Networking*, 2023(1), 36.

17. Nita, S. L., & Mihailescu, M. I. (2023). Elliptic curve-based query authentication protocol for IoT devices aided by blockchain. *Sensors*, 23(3), 1371.
18. Bae, W. I., & Kwak, J. (2020). Smart card-based secure authentication protocol in multi-server IoT environment. *Multimedia Tools and Applications*, 79(23), 15793-15811.
19. Siddhartha, V., Gaba, G. S., & Kansal, L. (2020). A lightweight authentication protocol using implicit certificates for securing IoT systems. *Procedia computer science*, 167, 85-96.
20. Thakare, A., & Kim, Y. G. (2021). Secure and efficient authentication scheme in IoT environments. *Applied Sciences*, 11(3), 1260.
21. Kang, B., Han, Y., Qian, K., & Du, J. (2020). Analysis and Improvement on an Authentication Protocol for IoT-Enabled Devices in Distributed Cloud Computing Environment. *Mathematical Problems in Engineering*, 2020(1), 1970798.
22. Taher, B. H., Liu, H., Abedi, F., Lu, H., Yassin, A. A., & Mohammed, A. J. (2021). A Secure and Lightweight Three-Factor Remote User Authentication Protocol for Future IoT Applications. *Journal of Sensors*, 2021(1), 8871204.
23. Ayub, M. F., Mahmood, K., Kumari, S., & Sangaiah, A. K. (2021). Lightweight authentication protocol for e-health clouds in IoT-based applications through 5G technology. *Digital Communications and Networks*, 7(2), 235-244.
24. Badhib, A., Alshehri, S., & Cherif, A. (2021). A robust device-to-device continuous authentication protocol for the internet of things. *IEEE Access*, 9, 124768-124792.
25. Mahmood, M. J. A., & Guin, U. (2020). A robust, low-cost and secure authentication scheme for IoT applications. *Cryptography*, 4(1), 8.
26. Jiang, L., & Cui, H. (2023). Private and mutual authentication protocols for internet of things. *Mathematics*, 11(8), 1929.
27. Shafiq, A., Ayub, M. F., Mahmood, K., Sadiq, M., Kumari, S., & Chen, C. M. (2020). An Identity-Based Anonymous Three-Party Authenticated Protocol for IoT Infrastructure. *Journal of Sensors*, 2020(1), 8829319.
28. Bułat, R., & Ogiela, M. R. (2023). Personalized context-aware authentication protocols in IoT. *Applied Sciences*, 13(7), 4216.
29. Tanveer, M., Chelloug, S. A., Alabdulhafith, M., & Abd El-Latif, A. A. (2024). Lightweight authentication protocol for connected medical IoT through privacy-preserving access. *Egyptian Informatics Journal*, 26, 100474.
30. Wu, T. Y., Meng, Q., Kumari, S., & Zhang, P. (2022). Rotating behind security: A lightweight authentication protocol based on iot-enabled cloud computing environments. *Sensors*, 22(10), 3858.