Journal of Information Systems Engineering and Management
2025, 10(15s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Analytical Study of Authentication and Lightweight Security Techniques in 5G-Enabled IoT Networks

Vyshali Rao K P[1] *Shanthi M B*[2] *Manoj Challa*[3]
1 Research Scholar, VTU-RC CMR Institute of Technology. Bengaluru, India.
Assistant Professor, JSS Science and Technological, University, Mysore, India, raovyshali@gmail.com
2 *Professor, Department of AI&DS, CMR Institute of Technology Bengaluru, India* shanthi.mb@cmrit.ac.in
3 *Professor, Department of CSE, Gopalan College of Engineering and Management, Bengaluru, India. manojreddi@gmail.com*

ARTICLE INFO

Received: 04 Dec 2024

Revised: 26 Jan 2025

Accepted: 05 Feb 2025

ABSTRACT

This study presents a comparative analysis of authentication mechanisms and lightweight security solutions within 5G-enabled IoT networks. With the advent of 5G technology, the proliferation of IoT devices necessitates robust yet efficient security protocols to safeguard sensitive data transmissions. We analyzed various authentication methods, including certificate-based, identity-based, and biometric-based authentication, to evaluate their effectiveness in providing secure and scalable solutions. Additionally, lightweight security protocols such as Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), and SHA-3 were assessed for suitability in resource-constrained IoT environments. We also examined post-quantum cryptographic approaches, including lattice-based cryptography and code-based cryptography, to address future quantum threats. The findings reveal that while traditional authentication methods ensure robust security, lightweight security solutions and post-quantum cryptographic approaches are essential for practical deployment in IoT devices with limited computational capabilities. This research highlights the importance of a tailored security approach in 5G IoT networks, balancing the diverse requirements of IoT devices with the critical need for efficient and secure data transmission. Ultimately, the study underscores the significance of selecting appropriate security mechanisms to achieve a harmonious blend of security and efficiency in 5G IoT deployments.

Keywords: User Equipment (UE), Subscription Identifier (SUPI), Home Network Public Key (HNPK), Authentication and Key Agreement (AKA), Extensible Authentication Protocol (EAP), Datagram Transport Layer Security (DTLS), Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), Lightweight Machine to Machine (LwM2M), Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD).

INTRODUCTION

The emergence of fifth-generation (5G) wireless technology represents a significant advancement in the Internet of Things (IoT), bringing unparalleled improvements in speed, capacity, and connectivity. This technological breakthrough is anticipated to drive substantial growth in IoT implementations, fostering innovations across sectors such as healthcare, transportation, smart cities, and agriculture. [1] However, the increased connectivity of these devices brings significant security challenges, necessitating the creation and deployment of advanced authentication and security frameworks to ensure the integrity, confidentiality, and availability of IoT networks and data. 5G networks offer several key enhancements over previous generations, including substantially higher data rates, dramatically reduced latency, and the capability to connect a large number of devices simultaneously [2]. These features make 5G the ideal infrastructure for IoT, enabling real-time communication and the implementation of advanced applications that were previously unattainable [3]. However, these same features also expand the attack surface, making the network more vulnerable to sophisticated cyber threats. In the context of IoT, robust security mechanisms are essential due to the sensitive nature of the data produced and transmitted by these devices [4]. Unauthorized access, data breaches, and manipulation of IoT data can lead to serious consequences, such as privacy

violations, operational disruptions, and threats to human safety. Therefore, developing comprehensive authentication and security schemes is critical to protecting the IoT ecosystem. Authentication in 5G-enabled IoT environments involves verifying the identities of devices and users to ensure that only authorized entities can access network resources [5]. This process is complicated by the heterogeneous nature of IoT devices, which vary widely in processing power, energy resources, and communication capabilities. Techniques like ECOA algorithm [6] optimizes energy consumption in 5G networks efficiently. Densified cell deployment in 5G increases network capacity and coverage [7]. Consequently, authentication mechanisms must be both lightweight and robust, adaptable to different device capabilities, and scalable to accommodate the vast number of devices expected in 5G networks. [8] Beyond authentication, extensive security measures must be implemented to protect IoT data and infrastructure. These measures include employing advanced encryption techniques [9] to safeguard data in transit and at rest, deploying intrusion detection systems to identify and mitigate potential threats, and utilizing secure boot mechanisms to ensure the integrity of device firmware [10]. Additionally, network slicing, a crucial feature of 5G, allows for the creation of isolated virtual networks tailored to specific IoT applications, providing an extra layer of security by segregating critical services from less sensitive ones [11].

AUTHENTICATION IN 5G NETWORKS

Primary authentication within 5G networks is facilitated by either the 5G-AKA or the EAP-AKA' (Extensible Authentication Protocol Method [12] [13] for 3rd Generation Authentication and Key Agreement). These protocols underpin the mutual verification processes between the UE and the network, ensuring robust authentication. The 5G Authentication and Key Agreement (AKA) protocol [14] [15] represents an evolution from its 4G LTE predecessor, designed to enhance security features and mitigate emerging threats. This protocol is pivotal for achieving mutual authentication between the user equipment (UE) and the network infrastructure. Subscription Identifier (SUPI) and Home Network Public Key (HNPK) [16] are the key authentication components in 5G cellular networks. The Subscription Permanent Identifier (SUPI) functions as a persistent identifier for the user, akin to the IMSI in 4G networks. To preserve user privacy, the SUPI is frequently obfuscated through the use of a Subscription Concealed Identifier (SUCI) during transmission. The Home Network Public Key (HNPK) is employed in the process of SUPI concealment, thereby safeguarding user privacy during communication.

There are different authentication protocol in 5G cellular telephony which are described in brief as:

• The 5G-AKA procedure is a critical authentication mechanism within 5G networks, ensuring secure and mutual authentication between the user equipment (UE) and the network. It begins with the UE sending an initial registration request to the Serving Network (SN), which then forwards the request to the Home Network (HN). The HN generates an authentication vector (AV) with the following mathematical model and sends it back to the SN.

$$AK=f(K, RAND)$$

$$SQN_{HN} = SQN \oplus AK$$

$$MAC=f(K, SQN_{HN}, RAND)$$

$$AUTN = SQN_{HN} \parallel MAC$$

Where, AK: Anonymity Key, K: Shared Secret Key, RAND: Random Number, SQN: Sequence Number, f: Cryptographic functions, AUTN: Authentication Token. The SN challenges the UE using the AV by computing with following model, and the UE responds accordingly.

$$AK=f5(K, RAND)$$

$$SQN_{UE} = SQN \oplus AK$$

$$MACUE = f1(K, SQNUE, RAND)$$

$$\text{Verify if } MAC_{UE} = MAC$$

Successful verification of the UE's response by the SN completes the mutual authentication process, establishing a secure communication channel.

• The 5G EAP-AKA' (Extensible Authentication Proto col Method for 3rd Generation Authentication and Key Agreement) [17] procedure is a vital authentication protocol used primarily for non-3GPP access, such as Wi Fi

networks. This method extends the traditional EAP framework to provide mutual authentication between the user equipment (UE) and the network. The process [18] begins with an EAP request from the network, followed by a response from the UE containing its identity. The Home Network (HN) then generates authentication vectors and sends an EAP challenge to the UE. The UE responds, and if the response is verified successfully, mutual authentication is achieved, ensuring a secure communication channel. This mechanism is similar to AKA model but authentication happen with in EAP framework providing more flexibility [19] and integration with various network environments, adding additional steps for identity management and communication. • EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) [20] is a sophisticated authentication protocol that employs Public Key Infrastructure (PKI) to ensure a high level of security and integrity in network communications. This protocol necessitates mutual authentication through the exchange of digital certificates between the client (user equipment, UE) and the server (network). In the EAP-TLS authentication process [21] [22], the UE initially presents its digital certificate to the network, which verifies the certificate's validity using the issuer's public key. Concurrently, the network provides its own digital certificate to the UE, which the UE verifies in a similar manner. This bidirectional certificate verification process establishes mutual trust between the communicating entities. Upon successful validation of certificates, a secure, encrypted communication channel is established, leveraging TLS to protect the integrity and confidentiality of the data exchanged. EAP-TLS is particularly advantageous in environments where security is paramount, such as enterprise networks, financial institutions, and other critical infrastructures. Its reliance on asymmetric cryptography and the robustness of PKI makes it a preferred choice for scenarios demanding stringent security measures and resilience against potential threats.

A. Comparison and sustainability

- 5G-AKA: Best for scenarios requiring standardized, network-level security in 3GPP networks. Suitable for high-security, large-scale IoT deployments in smart cities and critical infrastructure.
- EAP-AKA': Ideal for IoT devices needing flexible network access, including non-3GPP networks. Suitable for consumer IoT devices in smart homes and wearable's requiring seamless roaming and secure connectivity.
- EAP-TLS: Most suitable for applications demanding the highest security levels, utilizing certificates and PKI. Ideal for financial, medical, and critical infrastructure applications where data integrity and confidentiality are critical.

While 5G-AKA, EAP-AKA, and EAP-TLS offer robust authentication mechanisms, they also come with certain limitations and challenges [23] [24] when applied to IoT environments:

- IoT devices often have limited processing power, memory, and battery life. Implementing complex authentication protocols like 5G-AKA and EAP-TLS may strain these resources, leading to performance degradation and reduced device lifespan. [25] [26]. The additional computational and communication overhead required for authentication can increase latency and energy consumption, particularly in low-power IoT devices. • In scenarios involving massive deployments of IoT devices, such as smart cities or industrial IoT, traditional authentication protocols may struggle to scale efficiently. This lead to scalability issue. [27] [28]. The overhead of establishing and managing authentication sessions for a large number of devices can overwhelm the network infrastructure.
- The IoT ecosystem comprises a wide array of devices from different manufacturers, each with its own authentication capabilities and requirements [29]. Ensuring interoperability between devices using different authentication protocols like 5G-AKA, EAP-AKA, and EAP-TLS can be complex and may require additional standardization efforts.
- Traditional authentication protocols like 5G-AKA and EAP-TLS rely heavily on centralized entities, such as authentication servers and certificate authorities. A compromise of these centralized components could lead to widespread security breaches across the IoT network [30]. These protocols are highly vulnerable, so IoT devices may become targets for sophisticated attacks aimed at exploiting weaknesses in these protocols. Table 1 shows detailed view of these comparisons.

Table 1: A Comparative Analysis of 5G and IoT Authentication Mechanisms

Feature	**5G Authentication Protocols**	**IoT Authentication Protocols**
Mutual Authentication	✓(Between UE and Network)	✓(Device-to-Network and Device-to-Device)
Standardization	✓(3GPP Standardized)	(Varies Depending on Protocol)

Flexibility	X (Standardized Protocol)	✓(Diverse Range of Protocols)
Resource Consumption	Moderate to High	Low to Moderate
Scalability	Moderate to High	High (Depending on Protocol)
Interoperability	Moderate to High (Within 3GPP Networks)	Moderate (Varies Depending on Protocol)
Security Guarantees	Strong	Varies (Depends on Protocol)
Complexity	Moderate to High	Low to High (Depending on Protocol)
Suitable for Cellular IoT	✓(Well-Suited)	✓(Depends on Protocol)
Suitable for Non-Cellular IoT	X (Limited)	✓(EAP-AKA', Lightweight Protocols)
Certificate-Based Authentication	X (Except EAP-TLS)	✓(EAP-TLS, PKI Based Protocols)
Lightweight Authentication Protocols	X (Except Lightweight EAP Methods)	✓(DTLS, ECC, Lightweight Methods)
Group-Based Authentication	X	✓(GDOI, LwM2M, Group Authentication)
Public Key Infrastructure (PKI)	X (Limited to EAP-TLS)	✓(EAP-TLS, PKCIoT, PKI Based Methods)

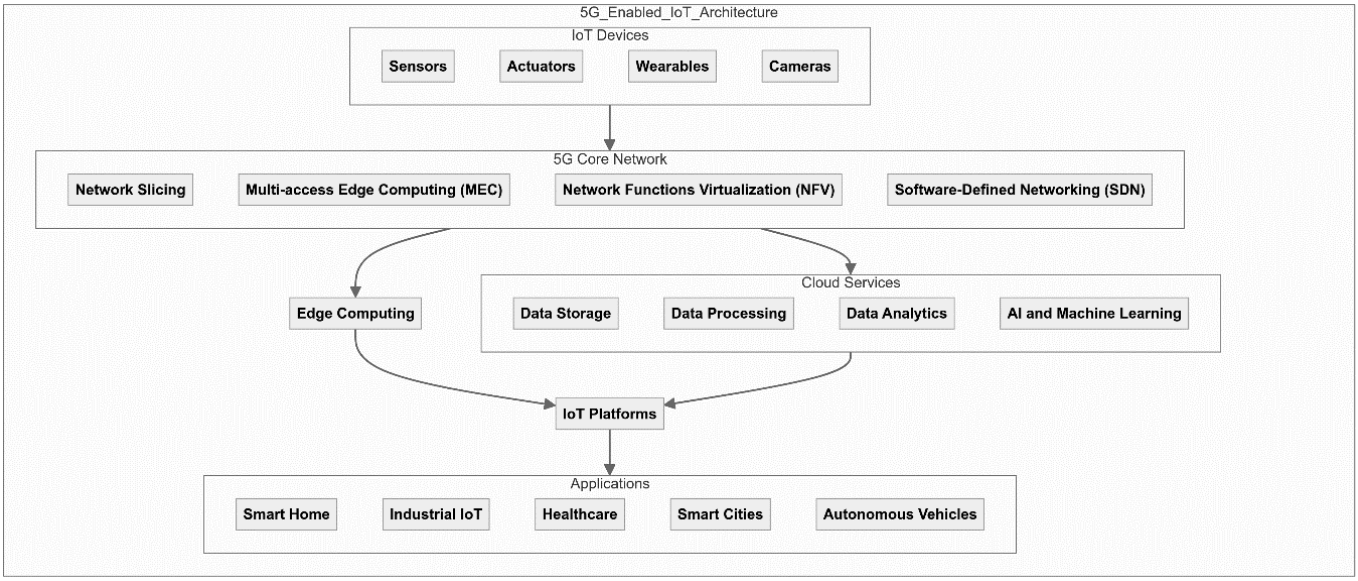

Fig. 1. Overall view of 5G enabled IoT Architecture

AUTHENTICATION IN IOT NETWORK

The Fig 1 describes various components involved in 5G enabled IOT Architecture.

- IoT Devices Block: This block contains all the IoT devices such as sensors, actuators, wearables, and cameras.
- 5G Core Network Block: This block represents the core functionalities of the 5G network including Network Slicing, MEC, NFV, and SDN.
- Edge Computing Block: This block represents the edge computing resources positioned close to IoT data sources. • Cloud Services Block: This block contains cloud-based services for data storage, processing, analytics, and AI/ML.
- IoT Platforms Block: This block represents the platforms that manage IoT devices and data.
- Applications Block: This block includes various applications that use IoT data, such as Smart Home, Industrial IoT, Healthcare, Smart Cities, and Autonomous Vehicles. In the current landscape of IoT, where devices frequently contend with limitations in resources and diverse communication methods, the choice of authentication protocols holds significant weight [31]. Presented below are various authentication protocols

commonly found in IoT environments, each meticulously designed to meet the unique needs of constrained devices:

- DTLS (Datagram Transport Layer Security): DTLS, a derivative of the TLS protocol, is meticulously crafted to surmount the challenges posed by unreliable datagram based communications, notably over UDP [46]. Serving as a bastion of secure communication and authentication, DTLS exemplifies an indispensable facet of IoT frameworks, particularly where minimized overhead and unwavering reliability are pivotal.
- MQTT (Message Queuing Telemetry Transport): Rep resenting a lightweight messaging protocol ubiquitously harnessed in IoT infrastructures, MQTT stands as a linchpin for inter-device and device-to-server communications [44]. Offering a spectrum of authentication modalities, including username/password-based authentication and TLS-driven mutual authentication, MQTT engenders a milieu of secure and authenticated discourse between its clients and brokers.
- CoAP (Constrained Application Protocol): Tailored explicitly for resource-constrained IoT devices, CoAP serves as a beacon of efficiency within the IoT pantheon [47]. In tandem with DTLS, CoAP orchestrates secure and authenticated exchanges, empowering devices to transact data securely with servers or proxies over UDP or SMS channels.
- OAuth 2.0: As an architectural cornerstone of delegated access control in IoT ecosystems, OAuth 2.0 [48] epitomizes a paradigm shift in authorization frameworks. Facilitating the granular acquisition of limited resource access sans divulging sensitive credentials, OAuth 2.0 stands poised to mitigate security concerns inherent in multifaceted IoT environments replete with diverse devices, services, and users.
- LwM2M (Lightweight M2M): Within the realm of IoT device management, LwM2M reigns supreme as a conduit for orchestrating secure interactions between devices and management platforms [45]. Encompassing security facets such as DTLS-based authentication and encryption, LwM2M embodies a sophisticated yet lightweight approach to fortifying communications in IoT ecosystems. Characterized by resource-constrained devices.
- SPAKE2: Addressing the exigencies of secure key exchange in IoT settings bereft of pre-shared keys, SPAKE2 emerges as an elegant solution [49]. Through a judicious blend of lightweight cryptography and robust authentication mechanisms, SPAKE2 empowers devices to authenticate one another and derive session keys clandestinely, thus ensuring the sanctity of communication channels sans the need to transmit sensitive credentials over the network. Table 2 and Table 3 shows a detailed view of these comparisons.

Table 2: Comparison of 5G and IoT Authentication Protocols

Feature/Protocol	**5G-AKA (Authentication and Key Agreement) (5G alone)**	**EAP-AKA' (Extensible Authentication Protocol - AKA') (5G alone)**	**MQTT (with TLS)(IOT Alone)**	**CoAP (with DTLS) (IOT Alone)**	**LwM2M (with DTLS) (IOT Alone)**
Authentication Type	Mutual Authentication [32]	Mutual Authentication [33]	Username/Password, Certificate [34]	PSK, RPK, X.509 Certificates [35]	PSK, RPK, X.509 Certificates [35]
Key Management	Home Subscriber Server (HSS) / Unified Data Management (UDM) [36] [37]	Home Subscriber Server (HSS) / UDM [36] [37]	Handled by TLS [38]	Handled by DTLS [39]	Handled by DTLS [39]
Encryption	Encryption between UE and network	Encryption between UE and network	TLS	DTLS	DTLS
Scalability	High [40]	High [40]	High [40] [41]	Moderate [42]	Moderate [43]
Overhead	Low to Moderate	Moderate	Low [44]	Low [44]	Low [45]
Complexity	High	High	Low to Moderate	Low to Moderate	Low to Moderate
Performance	High	High	High	High	High
Latency	Low	Low	Low	Low	Low
Use Case Suitability	Mobile and fixed devices, high-security requirements	Mobile and fixed devices, high-security requirements	Lightweight IoT devices, lower security	Constrained IoT devices, moderate security	Constrained IoT devices, device management
Implementation Difficulty	High	High	Low	Low	Low
Identity Protection	SUPI (Subscription Permanent Identifier), GUTI (Globally Unique Temporary Identifier)	SUPI, GUTI	Depends on implementation	Depends on implementation	Depends on implementation

The Pseudo code in Listing 1 above shows the authentication process using MQTT, DTLS, CoAP, OAuth, LwM2M, and SPAKE2.

Implementing IoT authentication protocols is fraught with challenges, including resource constraints for devices, complexity in implementation and management, and the potential for increased latency in real-time applications [50]. Scalability issues arise as traditional authentication mechanisms may struggle to accommodate the rapid expansion of IoT deployments, leading to scalability limitations or increased overhead [40]. Security vulnerabilities pose significant risks, exposing IoT devices and networks to various threats such as eavesdropping and data manipulation [51]. Achieving interoperability between diverse IoT devices, platforms, and authentication protocols is challenging due to the lack of standardized protocols and compatibility issues [52]. The overhead introduced by authentication processes consumes valuable network resources, potentially causing congestion or degraded performance. Addressing these challenges requires a comprehensive approach that considers device limitations, security needs, performance constraints, and interoperability issues. Striking a balance between security, efficiency, and usability is essential to ensure the resilience and effectiveness of IoT authentication mechanisms across diverse IoT ecosystems. In table I, various key features of 5G and IOT networks are analyzed.

```
// Device Initialization
function initializeDevice(D_i):
credentials_i = registerDeviceWithAuthorizationServer(D_i)

// OAuth Token Request
function requestOAuthToken(D_i, credentials_i):
T_i = authorizationServer.issueToken(credentials_i) return T_i

// MQTT/CoAP Connection function
connectToBroker(D_i, B, T_i):
B.verifyToken(T_i)
if B.isTokenValid(T_i):proceedToDTLSHandshake(D_i, B) else: denyAccess()

// DTLS Handshake with SPAKE2
function proceedToDTLSHandshake(D_i, B):
// Perform SPAKE2 for secure key exchange
K_s = SPAKE2.performKeyExchange(D_i, B)
If SPAKE2.isExchangeSuccessful():
 enableSecureCommunication(D_i, B, K_s)
else: terminateConnection()

// LwM2M Registration
function lwm2mRegister(D_i, server):
server.register(D_i, T_i)

// Secure Communication
function enableSecureCommunication(D_i, B, K_s):
while D_i.isConnectedTo(B):
message = D_i.prepareMessage()
encryptedMessage = encrypt(message, K_s)
B.receiveMessage(encryptedMessage)

// Main Process
function main():
D_i = initializeDevice("Device1")
T_i = requestOAuthToken(D_i, credentials_i)
lwm2mRegister(D_i, "LwM2MServer")
connectToBroker(D_i, "Broker", T_i)

main()
```

Listing 1. Pseudo code for IoT authentication using MQTT, DTLS, CoAP, OAuth, LwM2M, and SPAKE2

AUTHENTICATION IN 5G ENABLED IOT

Authentication in a 5G-enabled IoT network is crucial for ensuring the security and integrity of communications between devices, applications, and the network infrastructure. Major things that are under considerations are Device authentication, Network Authentication, User Authentication, Secure Key exchange. As we have seen drawbacks of 5G protocols when used in IOT environment, and IOT Protocols not compatible with 5G environment, exclusive

authentication protocols with little modifications are used in IOT environment. Few of such major authentication methods are listed in table III listing their features, advantages and challenges. 5G with IOT networks introduce enhanced authentication protocols to provide more robust security measures compared to previous generations. They heavily rely on SIM-based authentication [53], utilizing the Authentication and Key Agreement (AKA) protocol to verify the identity of devices. Multi-factor authentication (MFA) [54] becomes more prevalent in 5G, combining something you know (password), something you have (SIM card), and something you are (biometric data). Extensible Authentication Protocol (EAP) methods, such as EAP-AKA', are widely used in 5G networks for flexible and secure authentication. Additionally, 5G enables seamless authentication for IoT devices, ensuring secure communication and access management for billions of connected devices. The introduction of network slicing allows for the creation of multiple virtual networks with isolated security mechanisms tailored to specific applications. Zero trust principles are incorporated, requiring continuous verification of device and user identities, regardless of their location within or outside the network perimeter. Public Key Infrastructure (PKI) provides a framework for digital certificates and public-private key pairs to ensure secure communication. Token-based authentication protocols, such as OAuth 2.0, manage secure API access and facilitate seamless integration between different services. Emerging 5G authentication protocols are also exploring blockchain technology to create decentralized and tamper-proof authentication mechanisms, enhancing overall network security.

LIGHTWEIGHT SECURITY SCHEME IN 5G ENABLED IOT

In table 4, all available existing cryptographic algorithms are listed and their features of suitability are considered. Table 5 shows different algorithms and their vulnerabilities. This table helps us conclude that AES cryptographic algorithm with SHA-256 as hashing algorithm is the optimum solution for security concern in 5G enabled IOT with respect quantum attacks. Considering quantum attacks and threats, here are the few shortlisted quantum resistant algorithms. Table VI clearly compares various features of different cryptographic algorithms. While AES with SHA-256 is widely used and considered secure against classical attacks, it does have vulnerabilities to quantum attacks. Here are some cons of using AES with SHA-256 in the context of quantum attacks:

• Quantum Key Search: Grover's algorithm [74], a quantum algorithm, can reduce the effective key length of AES by half. While AES-256 provides a 256-bit key length, Grover's algorithm can effectively reduce this to 128 bits, compromising the security margin. The algorithm in 1, the Grover's algorithm is described for key search and collision search.

• Quantum Collision Search [71]: SHA-256, a widely used cryptographic hash function, is vulnerable to collision attacks with Grover's algorithm. While SHA-256 provides a 256-bit hash output, Grover's algorithm can find collisions with a complexity of 2^{128}, compromising data integrity.

• Quantum Speedup [63]: Quantum computers, once sufficiently developed, could provide a significant speedup for certain tasks, potentially making brute-force attacks on AES keys and collision searches on SHA-256 more feasible.

• Limited Key Size [68]: While AES with a 256-bit key is considered strong against classical attacks, the potential reduction in effective key size due to quantum attacks may necessitate the use of even larger key sizes to maintain security, leading to increased computational and memory requirements.

• Transition Challenges [72]: Transitioning to post-quantum cryptographic algorithms or larger key sizes may pose challenges in terms of compatibility, implementation complexity, and performance overhead, especially for existing systems and protocols that rely on AES with SHA-256.

• Long-Term Security [30]: As quantum computing continues to advance, the security of AES with SHA-256 may become increasingly uncertain in the long term, necessitating a transition to quantum-resistant algorithms or alternative cryptographic approaches.

Quantum computing poses a significant threat to traditional cryptographic mechanisms due to its ability to solve certain mathematical problems more efficiently than classical computers. This is especially relevant for 5G IoT networks, which require lightweight and efficient security solutions due to constraints on processing power, memory, and energy. To address these challenges, here are some lightweight security mechanisms for mitigating quantum attacks in 5G IoT:

• Post-Quantum Cryptography (PQC) Post-Quantum Cryptography aims to develop cryptographic algorithms that

are secure against both classical and quantum computers. Some lightweight PQC algorithms suitable for IoT devices include:

– Lattice-based Cryptography: Algorithms like NTRU and Ring-LWE offer strong security with relatively low computational requirements.

– Hash-based Cryptography: Merkle tree-based signature schemes such as SPHINCS+ provide stateless signatures that are quantum-resistant.

– Code-based Cryptography: Algorithms like McEliece and its variants offer resistance to quantum attacks with manageable key sizes and computational overhead.

- Lightweight Key Exchange Protocols Key exchange protocols must be both lightweight and quantum-resistant for use in 5G IoT networks. Examples include:

  – RLWE Key Exchange: Based on the Ring Learning with Errors problem, RLWE-based protocols provide quantum resistance with efficient computation.

  – NewHope: A key exchange protocol based on Ring LWE, designed to be efficient and quantum-resistant.

- Elliptic Curve Cryptography (ECC) on Twisted Edwards Curves While traditional ECC is vulnerable to quantum attacks, using twisted Edwards curves can still offer some efficiency advantages. Research is ongoing to make these curves more resistant to quantum attacks.

- Quantum Key Distribution (QKD) Integration Although QKD is not lightweight, integrating QKD with classical networks can enhance security. For IoT, this might involve leveraging QKD for key distribution in critical areas and using classical PQC for regular communications.

- Hybrid Cryptographic Systems combining classical cryptographic mechanisms with quantum-resistant algorithms can provide a transitional security measure. For instance:

  – Hybrid Key Exchange: Use a combination of ECDH (Elliptic Curve Diffie-Hellman) and RLWE-based key exchange to ensure security against both classical and quantum adversaries.

  – Hybrid Signatures: Use a combination of traditional digital signatures and post-quantum signatures to provide a fallback mechanism in case one is broken.

Table 3: Authentication in 5G Enabled IoT

Authentication Method	Description	Advantages	Challenges
SIM-based Authentication (AKA - Authentication and Key Agreement) [53] [55]	Uses the SIM card to authenticate devices to the network.	Highly secure, well-established, widely used in mobile networks.	Requires SIM cards, not suitable for all IoT devices.
EAP (Extensible Authentication Protocol) [12] [17]	Flexible authentication framework often used over Wi-Fi and cellular networks.	Supports various authentication methods, extensible.	Complexity in implementation, varies in security based on method used.
PKI (Public Key Infrastructure) [56]	Uses certificates and public-private key pairs to authenticate devices.	High security, widely trusted, non-repudiation.	Complex management, requires secure storage of private keys.
OAuth 2.0 [48] [57]	Token-based authentication protocol typically used for API security.	Scalable, does not require passwords, delegated access.	Token management complexity, initial setup can be complex.
DDA (Delegated Device Authentication) [43] [58]	Delegates authentication tasks to a trusted device or entity.	Reduces computational load on IoT devices, scalable.	Dependence on a trusted device, potential single point of failure.
Lightweight Machine to Machine (LwM2M) [45]	Protocol designed for remote management of M2M devices, includes security mechanisms.	Designed specifically for IoT, efficient.	May require updates to existing infrastructure, implementation complexity.
Blockchain-based Authentication [59] [14]	Uses blockchain technology to create a decentralized authentication system.	High security, tamper-resistant, decentralized.	High computational overhead, complex to implement.
Biometric Authentication [60]	Uses biometric data like fingerprints or facial recognition for authentication.	High security, user-friendly.	Privacy concerns, requires specialized hardware.
Token-based Authentication [61]	Uses tokens (e.g., JWT - JSON Web Tokens) to authenticate devices and users.	Stateless, scalable, widely adopted in web applications.	Token expiration and renewal, security of tokens.
Zero Trust Architecture [62]	Continuous verification of devices, regardless of their location within or outside the network perimeter.	High security, reduces risk of insider threats.	Implementation complexity, requires continuous monitoring.

Table 6: Comparison of AES, Lattice-based Cryptography, Hash-based Cryptography, and Code-based Cryptography

Attribute	AES (Advanced Encryption Standard)	Lattice-based Cryptography	Hash-based Cryptography	Code-based Cryptography
Type	Symmetric	Asymmetric	Asymmetric	Asymmetric
Quantum Vulnerability	Moderate (Grover's Algorithm)	Low	Low	Low
Quantum Resistance	Effective key length halved	Quantum-resistant	Quantum-resistant	Quantum-resistant
Efficiency	High	Moderate to High	Moderate	Moderate to Low
Key Sizes	128, 192, 256 bits	Larger (e.g., several kilobytes)	Variable (e.g., based on hash output size)	Large (e.g., tens to hundreds of kilobytes)
Encryption/Decryption Speed	Fast	Moderate	N/A (typically for signatures)	Moderate
Signature Size	N/A	Moderate to Large	Small to Moderate	Large
Public Key Size	N/A	Large (e.g., several kilobytes)	Small to Moderate	Large
Private Key Size	N/A	Small to Moderate	Small	Moderate
Typical Applications	Data encryption, VPNs, disk encryption	Secure communication, key exchange	Digital signatures, authentication	Secure communication, key exchange, encryption
Standard Algorithms	AES-128, AES-192, AES-256	NTRU, Ring-LWE, Kyber	SPHINCS+, Lamport-Diffie	McEliece, Classic McEliece
Strengths	Efficiency, well-established, hardware acceleration	Strong security, flexible, efficient	Stateless, strong security	Strong security, long-term confidence
Weaknesses	Key length needs doubling for quantum security	Larger key sizes, more complex implementations	Larger signature sizes, slower verification	Very large keys and ciphertexts
NIST PQC Status	Not part of PQC standardization	Multiple candidates (Kyber, NTRU)	Multiple candidates (SPHINCS+)	Classic McEliece under consideration

Algorithm 1 Grover's Algorithm

Initialization
Initialize n qubits to $|0\rangle^{\otimes n}$
Apply Hadamard transform $H^{\otimes n}$ to create a uniform superposition
$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$
Oracle Application
Apply Oracle U_f
$U_f|x\rangle = (-1)^{f(x)}|x\rangle$
After applying the oracle, the state is:
$|\psi_1\rangle = U_f |\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} (-1)^{f(x)}|x\rangle$
Amplitude Amplification
Apply Diffusion Operator D:
    Perform Hadamard transform $H^{\otimes n}$
    Apply inversion about average:
        Inversion = $2|\psi_0\rangle\langle\psi_0| - I$
    Perform Hadamard transform $H^{\otimes n}$ again
The Grover Operator G is:
    $G = DU_f$
Iteration
Repeat the Grover Operator G approximately k times:
    $k \approx \frac{\pi}{4}\sqrt{N}$
for i = 1 to k **do**
    Apply Grover Operator G
end for
Measurement
Measure the quantum state $|\psi\rangle$
With high probability, the measured state will be the marked item(s) =0

CONCLUSION

The study undertook a comprehensive analysis of authentication mechanisms and lightweight security solutions within 5G-enabled IoT networks, emphasizing the critical need for secure and efficient protocols tailored to resource-constrained environments. In-depth comparisons were made among various authentication methods, including certificate-based authentication, identity-based authentication, and biometric-based authentication. Each method's strengths and limitations were scrutinized, highlighting the necessity for robust and scalable authentication protocols

capable of addressing the unique challenges posed by IoT devices. Furthermore, the study evaluated lightweight security protocols such as Elliptic Curve Cryptography (ECC), Elliptic Curve Digital Signature Algorithm (ECDSA), and SHA-3. These protocols were assessed for their efficacy in balancing security requirements with the limited computational resources typical of IoT devices. The analysis demonstrated that while traditional authentication methods offer substantial security guarantees, lightweight security solutions present a viable alternative for scenarios where resource efficiency is paramount. In conclusion, the study illuminates the importance of strategic security mechanism selection to ensure that 5G IoT deployments can effectively harmonize robust security measures with the efficiency demands of resource-constrained devices.

CONFLICT OF INTEREST

Authors show no conflict of interest

REFRENCES

[1] Honnavalli Prasad, Eswaran and Sivaraman. Private 5g networks: a survey on enabling technologies, deployment models, use cases and research directions. Telecommunication Systems, 82(1), 2023.

[2] Seyed Salar Sefati and Simona Halunga. Ultra-reliability and low-latency communications on the internet of things based on 5g network: Literature review, classification, and future research view. Transactions on Emerging Telecommunications Technologies, 34(6):e4770, 2023.

[3] Ahmed Alkhayyat Badria Sulaiman Alfurhood D. Haritha Deevi Radha Rani M. Karthick Azath Mubarakali, Salomi Samsudeen. Optimized flexible network architecture creation against 5g communication-based iot using information-centric wireless computing. Springer Science+Business Media, LLC, part of Springer Nature 2023, https://doi.org/10.1007/s11276-023-03531-1(0123456789().,- volV)(0123456789(). ,- volV) 2023.

[4] Souhayla Dargaoui, Mourade Azrour, Ahmed El Allaoui, Fatima Amounas, Azidine Guezzaz, Hanaa Attou, Chaimae Hazman, Said Benkirane, and Sara Haddou Bouazza. An overview of the security challenges in iot environment. Advanced Technology for Smart Environment and Energy, pages 151–160, 2023.

[5] Manasha Saqib and Ayaz Hassan Moon. A systematic security assessment and review of internet of things in the context of authentication. Computers & Security, 125:103053, 2023

[6] Amjad Qtaish, Malik Braik, Dheeb Albashish, Mohammad T Alshammari, Abdulrahman Alreshidi, and Eissa Jaber Alreshidi. Enhanced coati optimization algorithm using elite opposition-based learning and adaptive search mechanism for feature selection. International Journal of Machine Learning and Cybernetics, pages 1–34, 2024.

[7] MOHAMMED FATTAH SAID MAZER MOULHIME EL BEKKALI AND AHMED D. KORA MACOUMBA FALL, YOUNES BALBOUL. Towards sustainable 5g networks: A proposed coordination solution for macro and pico cells to optimize energy efficiency. IEEE Access, 10.1109/ACCESS.2023.3278209, 2023.

[8] Ramiz Salama, Chadi Altrjman, and Fadi Al-Turjman. An overview of the internet of things (iot) and machine to machine (m2m) communications. NEU Journal for Artificial Intelligence and Internet of Things, 2(3), 2023.

[9] Firuz Kamalov, Behrouz Pourghebleh, Mehdi Gheisari, Yang Liu, and Sherif Moussa. Internet of medical things privacy and security: Challenges, solutions, and future trends from a new perspective. Sustainability, 15(4):3317, 2023.

[10] M Kokila and Srinivasa Reddy. Authentication, access control and scalability models in internet of things security-a review. Cyber Security and Applications, page 100057, 2024.

[11] Virendra Pratap Singh, Mahendra Pratap Singh, Saumya Hegde, and Maanak Gupta. Security in 5g network slices: Concerns and opportunities. IEEE Access, 2024.

[12] A DeKok. Rfc 9427: Tls-based extensible authentication protocol (eap) types for use with tls 1.3, 2023.

[13] Maroua Moatemri, Hamdi Eltaief, and Habib Youssef. Enhancing security in multi-controller sdmn environments: A novel 5g access authentication protocol. In 2024 International Wireless Communications and Mobile Computing (IWCMC), pages 993–998. IEEE, 2024.

[14] Awaneesh Kumar Yadav, Manoj Misra, Pradumn Kumar Pandey, Pasika Ranaweera, Madhusanka Liyanage, and Neeraj Kumar. A secure authentication protocol for iot-wlan using eap framework. IEEE Transactions on Dependable and Secure Computing, 2024.

[15] Teng Fei and Wenye Wang. The vulnerability and enhancement of aka protocol for mobile authentication in lte/5g networks. Computer Networks, 228:109685, 2023.

[16] Aditi Shukla, Fabian Sowieja, Axel Sikora, et al. Certificate based primary authentication for 5g networks. In 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), volume 1, pages 1223–1229. IEEE, 2023.
[17] Ilsun You, Gunwoo Kim, Seonghan Shin, Hoseok Kwon, Jongkil Kim, and Joonsang Baek. 5g-aka-fs: A 5g authentication and key agreement protocol for forward secrecy. Sensors, 24(1):159, 2023.
[18] Ruhui Ma, Jin Cao, Shiyang He, Yinghui Zhang, Ben Niu, and Hui Li. A uav-assisted ue access authentication scheme for 5g/6g network. IEEE Transactions on Network and Service Management, 2023.
[19] Souhayla Dargaoui, Mourade Azrour, Ahmad El Allaoui, Azidine Guezzaz, Abdulatif Alabdulatif, and Abdullah Alnajim. Internet of things authentication protocols: Comparative study. Computers, Materials & Continua, 79(1), 2024.
[20] Naiguang Zhu, Jie Xu, and Baojiang Cui. Formal analysis of 5g eap-tls 1.3. In International Conference on Emerging Internet, Data & Web Technologies, pages 140–151. Springer, 2024.
[21] Qianli Wang. Applying spin checker on 5g eap-tls authentication protocol analysis. Computer Science and Information Systems, 21(1):21– 36, 2024.
[22] Pooja Kumari and Ankit Kumar Jain. A comprehensive study of ddos attacks over iot network and their countermeasures. Computers & Security, 127:103096, 2023.
[23] Yahia Hasan Jazyah. 5g security, challenges, solutions, and authentication. International Journal of Advances in Soft Computing & Its Applications, 15(3), 2023.
[24] Jonathan Cook, Sabih Ur Rehman, and M Arif Khan. Security and privacy for low power iot devices on 5g and beyond networks: Challenges and future directions. IEEE Access, 11:39295–39317, 2023.
[25] Kishor Kumar Das, Mr Manoj Yadav, and Harsh Lohiya. A review on security challenges and future layout of iot in 5g network. networks, 8(9):10.
[26] Hussam N Fakhouri, Sadi Alawadi, Feras M Awaysheh, Imad Bani Hani, Mohannad Alkhalaileh, and Faten Hamad. A comprehensive study on the role of machine learning in 5g security: challenges, technologies, and solutions. Electronics, 12(22):4604, 2023.
[27] Smriti Sachan, Rohit Sharma, and Amit Sehgal. Energy efficiency and scalability of 5g networks for iot in mobile wireless sensor networks. In 5G and Beyond, pages 151–168. Springer Nature Singapore Singapore, 2023.
[28] Husam Rajab and Tibor Cinkler. Enhanced energy efficiency and scalability in cellular networks for massive iot. 5G and Beyond, page 283, 2023.
[29] Antonios Pliatsios, Konstantinos Kotis, and Christos Goumopoulos. A systematic review on semantic interoperability in the ioe-enabled smart cities. Internet of Things, 22:100754, 2023.
[30] Dalton CG Valadares, Newton C Will, Alvaro ´ A CC Sobrinho, Anna CD ´ Lima, Igor S Morais, and Danilo FS Santos. Security challenges and recommendations in 5g-iot scenarios. In International Conference on Advanced Information Networking and Applications, pages 558–573. Springer, 2023.
[31] Chi-Wei Lien and Sudip Vhaduri. Challenges and opportunities of biometric user authentication in the age of iot: A survey. ACM Computing Surveys, 56(1):1–37, 2023.
[32] Sudip Kumar Palit, Mohuya Chakraborty, and Subhalaxmi Chakraborty. Performance analysis of 5gmaka: lightweight mutual authentication and key agreement scheme for 5g network. The Journal of Supercomputing, 79(4):3902–3935, 2023.
[33] Mohammad Mahdi Modiri, Mahmoud Salmasizadeh, Javad Mohajeri, and Babak Hossein Khalaj. Two protocols for improving security during the authentication and key agreement procedure in the 3gpp networks. Computer Communications, 211:286–301, 2023.
[34] Mohammad Kamrul Hasan, Zhou Weichen, Nurhizam Safie, Fatima Rayan Awad Ahmed, and Taher M Ghazal. A survey on key agreement and authentication protocol for internet of things application. IEEE Access, 2024.
[35] Asier Atutxa Imatz, Jasone Astorga Burgo, Marc Barcelo, Aitor Urbi- ´ eta Aizpurua, and Eduardo Jacob. Improving efficiency and security of iiot communications using in-network validation of server certificate. 2023.
[36] Zakaria Benfarhi. Evaluation of a new authentication and key agreement protocol for 5g network. 2024.
[37] Jinhui Li, Chengbin Huang, and Jinhua Wang. An enhanced application authentication and key management in 5g. In Journal of Physics: Conference Series, volume 2625, page 012071. IOP Publishing, 2023.
[38] Iqbal Luqman Bin Mohd Paris, Mohamed Hadi Habaebi, and Alhareth Mohammed Zyoud. Implementation of ssl/tls security with mqtt protocol in iot environment. Wireless Personal Communications, 132(1):163–182, 2023.

[39] Mattia Giovanni Spina and Floriano De Rango. Lightweight, dynamic and energy efficient security mechanism for constrained iot devices using coap. In 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC), pages 1123–1128. IEEE, 2023.
[40] Mohammed Jouhari, Nasir Saeed, Mohamed-Slim Alouini, and El Mehdi Amhoud. A survey on scalable lorawan for massive iot: Recent advances, potentials, and challenges. IEEE Communications Surveys & Tutorials, 2023.
[41]] Noor Ul Arfeen, Javed Iqbal Bangash, Salman Ahmed, Waseem Ullah Khan, and Lala Rukh. Enhanced datagram transport layer security protocol for iot environment.
[42] Tse-Chuan Hsu. Designing a secure and scalable service agent for iot transmission through blockchain and mqtt fusion. Applied Sciences, 14(7):2975, 2024.
[43] Donggyu Kim, Uk Jo, Yohan Kim, Yustus Eko Oktian, and Howon Kim. Design and implementation of a blockchain based interworking of onem2m and lwm2m iot systems. Journal of Information Processing Systems, 19(1), 2023.
[44] Sujitha Lakshminarayana, Amit Praseed, and P Santhi Thilagam. Securing the iot application layer from an mqtt protocol perspective: Challenges and research prospects. IEEE Communications Surveys & Tutorials, 2024.
[45] Radim Dvorak, Lukas Jabloncik, Michal Mikulasek, Martin Stusek, Pavel Masek, Radek Mozny, Aleksandr Ometov, Petr Mlynek, Petr Cika, and Jiri Hosek. Lwm2m for cellular iot: Protocol implementation and performance evaluation. In 2023 15th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), pages 212–218. IEEE, 2023.
[46] A Sara and J Randa. Data protection in iot using coap based on enhanced dtls. In AIP Conference Proceedings, volume 2729. AIP Publishing, 2024.
[47] Pritam S Salankar, Vinay Avasthi, and Ashutosh Pasricha. Lightweight authentication scheme based on modified eap security for coap protocolbased iomt applications. International Journal of Information and Computer Security, 20(1-2):176–198, 2023.
[48] Shrabani Sutradhar, Sunil Karforma, Rajesh Bose, Sandip Roy, Sonia Djebali, and Debnath Bhattacharyya. Enhancing identity and access management using hyperledger fabric and oauth 2.0: A block-chainbased approach for security and scalability for healthcare industry. Internet of Things and Cyber-Physical Systems, 4:49–67, 2024.
[49] T Taubert and CA Wood. Rfc 9383: Spake2+, an augmented passwordauthenticated key exchange (pake) protocol, 2023.
[50] MR Poornima, HS Vimala, and J Shreyas. Holistic survey on energy aware routing techniques for iot applications. Journal of Network and Computer Applications, 213:103584, 2023.
[51] Jean-Paul A Yaacoub, Hassan N Noura, Ola Salman, and Ali Chehab. Ethical hacking for iot: Security issues, challenges, solutions and recommendations. Internet of Things and Cyber-Physical Systems, 3:280–308, 2023.
[52] Christof Koolen. Interoperability in iot ecosystems. Available at SSRN 4474625, 2023.
[53] Siddharth Prakash Rao and Alexandros Bakas. Authenticating mobile users to public internet commodity services using sim technology. In Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks, pages 151–162, 2023.
[54] Zigang Chen, Zhiquan Cheng, Wenjun Luo, Jin Ao, Yuhong Liu, Kai Sheng, and Long Chen. Fsmfa: Efficient firmware-secure multi-factor authentication protocol for iot devices. Internet of Things, 21:100685, 2023.
[55] Hemangi Goswami and Hiten Choudhury. An esim-based remote credential provisioning and authentication protocol for iot devices in 5g cellular network. Internet of Things, 23:100876, 2023.
[56] Baiji Hu, Jingyi Cao, Ziqing Lin, Yayun Zhu, Dong Liang, Xiaojuan Zhang, and Han Liu. Lightweight iot-based authentication scheme in 5g circumstance. In 2023 4th International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), pages 395–398. IEEE, 2023.
[57] Sujeet Raosaheb Suryawanshi, Prashant B Kumbharkar, and Shailesh Kumar. Self-sovereign identity approach in oauth 2.0. 2023.
[58] Taehoon Kim, Daehee Seo, Su-Hyun Kim, and Im-Yeong Lee. A comprehensive approach to user delegation and anonymity within decentralized identifiers for iot. Sensors, 24(7):2215, 2024.
[59] Abba Garba, David Khoury, Patrick Balian, Samir Haddad, Jinane Sayah, Zhong Chen, Zhi Guan, Hani Hamdan, Jinan Charafeddine, and Khalid Al-Mutib. Lightcert4iots: Blockchain-based lightweight certificates authentication for iot applications. IEEE Access, 11:28370– 28383, 2023.

[60] Taha Beyrouthy, Nour Mostafa, Ahmed Roshdy, Abdullah S Karar, and Samer Alkork. Review of eeg-based biometrics in 5g-iot: Current trends and future prospects. Applied Sciences, 14(2):534, 2024.

[61] Xutong Jiang, Ruihan Dou, Qiang He, Xuyun Zhang, and Wanchun Dou. Edgeauth: An intelligent token-based collaborative authentication scheme. Software: Practice and Experience, 2023.

[62] Claudio Zanasi, Silvio Russo, and Michele Colajanni. Flexible zero trust architecture for the cybersecurity of industrial iot infrastructures. Ad Hoc Networks, page 103414, 2024.

[63] Miralem Mehic, Libor Michalek, Emir Dervisevic, Patrik Burdiak, Matej Plakalovic, Jan Rozhon, Nerman Mahovac, Filip Richter, Enio Kaljic, Filip Lauterbach, et al. Quantum cryptography in 5g networks: A comprehensive overview. IEEE Communications Surveys & Tutorials, 2023.

[64] Imran Makhdoom, Mehran Abolhasan, Daniel Franklin, Justin Lipman, Christian Zimmermann, Massimo Piccardi, and Negin Shariati. Detecting compromised iot devices: Existing techniques, challenges, and a way forward. Computers & Security, 132:103384, 2023.

[65] Ajay Kaushik, Lakshmi Sai Srikar Vadlamani, Mohammed Mohsin Hussain, Milind Sahay, Rahul Singh, Ananya Komal Singh, S Indu, Puneet Goswami, and Nalliyanna Goundar Veerappan Kousik. Post quantum public and private key cryptography optimized for iot security. Wireless Personal Communications, 129(2):893–909, 2023.

[66] Ishu Gupta, Ankit Tiwari, Priya Agarwal, Sloni Mittal, and Ashutosh Kumar Singh. Dodging security attacks and data leakage prevention for cloud and iot environments. In Intelligent Analytics for Industry 4.0 Applications, pages 209–232. CRC Press, 2023.

[67] Sarah Ahmed and Muhammad Khan. Securing the internet of things (iot): A comprehensive study on the intersection of cybersecurity, privacy, and connectivity in the iot ecosystem. AI, IoT and the Fourth Industrial Revolution Review, 13(9):1–17, 2023.

[68] V Thirunavukkarasu, A Senthil Kumar, P Prakasam, and G Suresh. Elliptic curve cryptography based key management and flexible authentication scheme for 5g wireless networks. Multimedia Tools and Applications, 82(14):21131–21145, 2023.

[69] Shreeya Swagatika Sahoo, Sujata Mohanty, Kshira Sagar Sahoo, Mahmoud Daneshmand, and Amir H Gandomi. A three factor based authentication scheme of 5g wireless sensor networks for iot system. IEEE internet of things journal, 2023.

[70] Alvaro Michelena, Jose Aveleira-Mata, Esteban Jove, Mart ´ ´ın Bayon- ´ Gutierrez, Paulo Novais, Oscar Fontenla Romero, Jos ´ e Luis Calvo-Rolle, ´ and Hector Al ´ aiz-Moret ´ on. A novel intelligent approach for man-in-the- ´ middle attacks detection over internet of things environments based on message queuing telemetry transport. Expert Systems, 41(2):e13263, 2024.

[71] Zeyad Ghaleb Al-Mekhlafi, Mahmood A Al-Shareeda, Selvakumar Manickam, Badiea Abdulkarem Mohammed, and Amjad Qtaish. Lattice-based lightweight quantum resistant scheme in 5g-enabled vehicular networks. Mathematics, 11(2):399, 2023.

[72] Saurabh Bhatt, Bharat Bhushan, Tanya Srivastava, and VS Anoop. Post-quantum cryptographic schemes for security enhancement in 5g and b5g (beyond 5g) cellular networks. In 5G and Beyond, pages 247–281. Springer Nature Singapore Singapore, 2023.

[73] Justin Kinney. Analyzing insider risk threat to the internet of things (iot). Technical report, Oak Ridge National Laboratory (ORNL), Oak Ridge, TN (United States), 2023.

[74] Muhammad Idham Habibie, Claire Goursaud, et al. Quantum minimum searching algorithms for active user detection in wireless iot networks. IEEE Internet of Things Journal, 2024