A Review on Advancing Authentication Mechanisms: Integrating Physical Layer Security, Machine Learning, and Scalable Solutions

Shen Qian

Department of Science and Technology, Faculty of Science and Technology, Seikei University, Tokyo, Japan
Email: shen-qian@st.seikei.ac.jp

***Abstract*—Authentication mechanisms are pivotal for ensuring secure communication in modern network environments, which are characterized by increasing complexity and heterogeneity, such as wireless networks, the Internet of Things (IoT), and Visible Light Communication (VLC). This paper presents a comprehensive review of contemporary authentication techniques, focusing on the integration of Physical Layer Security (PLS), Machine Learning (ML), and scalable cryptographic solutions to address evolving security challenges. The study categorizes authentication approaches into cryptographic-based, biometric-based, and PLS-enhanced methods, analyzing their principles, strengths, and limitations. Key advancements include the application of Multiple Input Multiple Output (MIMO) and cooperative relaying in wireless networks for mitigating eavesdropping and supporting high-mobility scenarios. In VLC systems, innovative solutions such as "Optic Fingerprints" and nanomaterial-based enhancements leverage unique physical-layer properties to strengthen authentication. Additionally, scalable and lightweight protocols, incorporating technologies like Physical Unclonable Functions (PUFs) and TinyML, are proposed to address the constraints of resource-limited IoT devices and massive network deployments. This paper highlights critical challenges, including the trade-offs between computational efficiency and security, scalability in dense networks, and the transition to quantum-resistant authentication mechanisms. By adopting a multidisciplinary approach, this study offers insights into developing adaptive and robust authentication frameworks that align with the demands of next-generation networks. The findings underscore the need for collaborative research and standardization to ensure the seamless deployment of secure and efficient authentication systems.**

***Keywords*—authentication mechanisms, Physical Layer Security (PLS), Machine Learning (ML), Internet of Things (IoT), Visible Light Communication (VLC)**

I. Introduction

In the era of pervasive connectivity and digitization, authentication is a cornerstone of network security, ensuring information integrity, confidentiality, and availability across diverse communication systems. As modern networks expand to include billions of connected devices, verifying identities and establishing trust in these systems has become increasingly critical. Authentication mechanisms are pivotal in safeguarding sensitive data and enabling secure and reliable interactions in applications ranging from smart homes and autonomous vehicles to industrial Internet of Things (IoT) and next-generation networks [1].

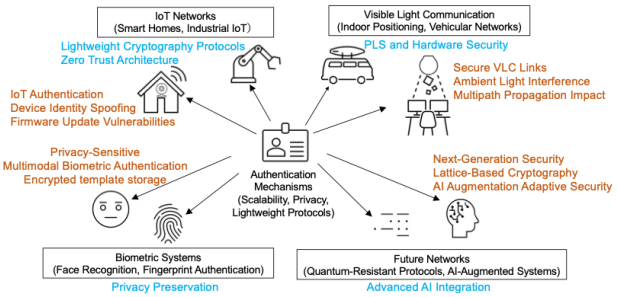

Fig. 1. Application scenarios of advanced authentication mechanisms.

However, the growing heterogeneity of network environments introduces significant challenges to traditional authentication approaches. For example, in resource-constrained IoT devices, achieving a balance between lightweight security and computational efficiency remains an ongoing struggle [2]. Similarly, the high mobility and rapid topology changes inherent in 5G and vehicular networks complicate the implementation of real-time authentication protocols. Emerging technologies such as Visible Light Communication (VLC) add further complexity by introducing unique physical-layer characteristics that require novel solutions to address security and scalability concerns [3]. These challenges necessitate a shift toward adaptive, scalable, and resource-efficient authentication mechanisms tailored to the specific needs of each environment.

To address these gaps, this paper aims to provide a comprehensive overview of recent advancements in authentication mechanisms, focusing on their applications in specialized network environments [4]. Fig. 1 illustrates the diverse application areas of authentication mechanisms, ranging from IoT and VLC to biometric systems and future networks. Each scenario highlights a specific application with relevant security challenges and

Manuscript received January 11, 2025; revised February 10, 2025, accepted February 24, 2025; published April 17, 2025.

solutions. By examining cutting-edge technologies such as MIMO-enhanced wireless authentication, VLC-based security techniques, and scalable protocols for IoT, this work identifies the limitations. It equips researchers and practitioners with a holistic perspective on the future of authentication in modern, heterogeneous network environments.

The rest of this article is organized as follows: Section II presents a classification of authentication mechanisms based on their foundational principles, distinguishing between cryptographic approaches and Physical Layer Security (PLS)-enhanced techniques. This section examines the strengths, limitations, and emerging trends in both symmetric and asymmetric cryptography, including advancements in post-quantum cryptographic schemes and hybrid encryption methods. Section III explores emerging trends in authentication, including the integration of machine learning for anomaly detection and adaptive authentication, decentralized authentication mechanisms using blockchain technology, and the transition to quantum-resilient cryptographic frameworks. Section IV delves into authentication mechanisms tailored for specialized network environments, such as wireless networks leveraging Multiple Input Multiple Output (MIMO) and cooperative relaying, authentication strategies for VLC based on unique optical properties, and lightweight security solutions for IoT and 6G networks. Section V outlines key challenges and future research directions, emphasizing the need for scalable, energy-efficient, and quantum-secure authentication solutions. Finally, Section VI concludes the paper by summarizing key findings and discussing the future landscape of authentication technologies in dynamic and heterogeneous network environments.

II. Classification of Authentication Schemes

As the demand for secure communication grows in the age of interconnected devices and networks, authentication mechanisms have become pivotal in ensuring data integrity, confidentiality, and system reliability. The diversity of authentication schemes reflects the wide range of challenges and requirements across different application scenarios, from resource-constrained IoT devices to quantum-resistant critical infrastructures [5]. This section explores the fundamental principles and practical implementations of authentication schemes, categorizing them into cryptographic methods, including symmetric and asymmetric approaches and Physical Layer Security (PLS)-enhanced techniques. Examining the latest advancements and use cases provides a comprehensive understanding of how these approaches address contemporary threats and enable secure interactions in dynamic and heterogeneous environments.

A. Principles of Symmetric and Asymmetric Cryptography

Cryptography continues to evolve to address the increasing complexities of modern communication systems. Symmetric encryption, such as the Advanced Encryption Standard (AES), remains a cornerstone due to its efficiency and speed. Recent advancements have focused on optimizing these algorithms for resource-constrained environments like IoT networks [6]. These optimizations ensure that even devices with limited computational power can maintain robust security.

In contrast, asymmetric cryptography has seen significant developments in response to the potential threats posed by quantum computing. Traditional algorithms like RSA and ECC are vulnerable to quantum attacks, prompting the development of post-quantum cryptographic schemes [7]. Lattice-based, hash-based, and code-based methods have emerged as promising candidates to ensure long-term security in the post-quantum era.

Hybrid encryption schemes, which combine the strengths of symmetric and asymmetric methods, have gained prominence in securing IoT communications. These approaches leverage the efficiency of symmetric encryption for data transfer and the robust key management capabilities of asymmetric cryptography [8]. Such schemes effectively address challenges related to key distribution and computational overhead in distributed systems. Table I provides a comparative analysis of symmetric and asymmetric cryptography, highlighting key differences in terms of key usage, speed, key management, security risks, and commonly used algorithms.

TABLE I. Comparison of Symmetric and Asymmetric Cryptography

	Symmetric Cryptography	**Asymmetric Cryptography**
Key Usage	Single key for encryption and decryption	Public key for encryption, private key for decryption
Speed	Fast, suitable for bulk data encryption	Slower, ideal for secure key exchange
Key Management	Complex in large networks	Simplified via public private key pairs
Security Risk	Compromised key affects all users	Compromised private key affects only one user
Common Algorithms	AES, DES, ChaCha20	RSA, ECC, ElGamal

B. Physical Layer Security-Enhanced Authentication

In recent years, the utilization of physical layer attributes, particularly Channel State Information (CSI) and Received Signal Strength Indicator (RSSI), has gained prominence in enhancing authentication mechanisms within wireless communication systems [9]. These methodologies offer inherent security advantages by exploiting the unique and location-specific characteristics of wireless channels.

Leveraging Physical Properties for Authentication: CSI provides detailed information about the channel's frequency response, while RSSI measures the power present in a received radio signal. By analyzing these parameters, systems can authenticate devices based on the distinctiveness of their physical transmission environments. Fig. 2 demonstrates the sequential steps

involved in leveraging physical layer attributes such as CSI and RSSI for device authentication.

Recent studies have demonstrated the efficacy of deep learning models in processing CSI data to accurately distinguish between legitimate users and potential intruders. For instance, a deep-CSI-based authentication scheme has been proposed to map CSI to a device's location and further to its authenticated identity via deep learning, eliminating the need for cryptography-based authentication in static environments [10].

PLS Against Eavesdropping and Spoofing Attacks: The dynamic nature of wireless channels makes it challenging for adversaries to replicate specific CSI or RSSI patterns, thereby providing a robust defense against eavesdropping and spoofing. Analytical methods have been developed to utilize channel phase information for physical layer authentication, effectively defending against such attacks [11]. Furthermore, the development of environment semantics-enabled physical layer authentication networks, such as EsaNet, has demonstrated robustness in time-varying wireless environments, effectively detecting spoofing attacks by capturing frequency-independent wireless channel fingerprints [12, 13].

AI on PLS-based Authentication: The convergence of machine learning techniques with physical layer authentication has led to significant improvements in system resilience. Notably, the application of deep neural networks enables the extraction of intricate features from CSI data, facilitating more accurate authentication processes. Additionally, the integration of graph neural networks has shown promise in detecting spoofing at the physical layer by analyzing RSSI features, enhancing the system's ability to identify unauthorized access attempts [14].

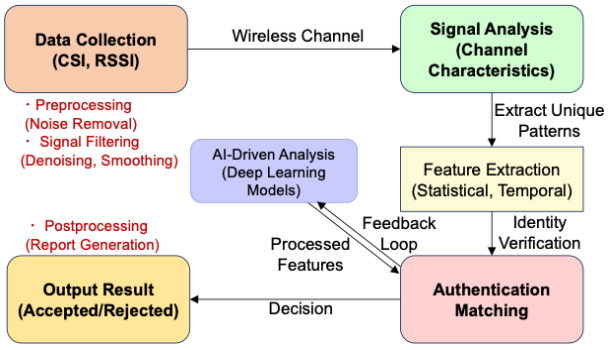

Fig. 2. PLS-based authentication workflow.

III. Emerging Trends in Authentication

The rapid evolution of digital technologies and the proliferation of connected devices have necessitated advancements in authentication mechanisms to address increasingly sophisticated security threats. As traditional methods face challenges such as scalability limitations, computational overhead, and vulnerability to emerging quantum computing threats, novel approaches are being developed to ensure robust and efficient authentication. This section delves into groundbreaking trends in authentication, including the integration of machine learning for adaptive security, the adoption of decentralized authentication frameworks, and the transition to quantum-resilient cryptographic systems. By exploring these innovations, we aim to highlight their potential applications, ongoing challenges, and future directions in safeguarding modern network infrastructures. Table II compares traditional and physical layer authentication, highlighting differences in security basis, quantum resistance, resource requirements, scalability, and adaptability to mobility.

A. Machine Learning-Driven Authentication

Machine Learning (ML) has revolutionized anomaly detection and adaptive authentication by enabling dynamic responses to evolving security threats. Recent advancements highlight its effectiveness in identifying anomalous behavior and enhancing authentication mechanisms with adaptive capabilities.

Anomaly Detection: ML techniques such as supervised, unsupervised, and semi-supervised learning have been employed to detect deviations from normal patterns in data. For instance, a machine learning-based system for network anomaly detection has been develops and validated in demonstrating its high accuracy and practical potential for identifying and addressing anomalies in complex network environments. [15]. Furthermore, the integration of deep learning approaches, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), has enabled the real-time detection of sophisticated anomalies in network traffic and user behavior [16].

Dynamic Authentication: Dynamic authentication leverages real-time contextual data to enhance security by continuously adapting authentication requirements based on user behavior, device usage patterns, and environmental factors. The approach employs advanced machine learning techniques, such as gradient boosting and reinforcement learning, to assess risk levels dynamically and adjust security measures accordingly. This ensures a seamless and secure user experience while mitigating threats like session hijacking and credential theft. Key features include real-time analysis of multimodal data, adaptive decision-making, and scalability for diverse applications, particularly in IoT and telehealth systems where traditional static methods are less effective [17].

Trade-offs Between Accuracy and Computational Overhead: While ML models improve detection and authentication accuracy, they introduce significant computational overhead, particularly in resource-constrained environments. To address this, lightweight ML models, such as TinyML, have been developed to operate efficiently on edge devices without compromising performance [18].

These developments highlight the potential of ML to enhance security mechanisms while addressing challenges related to computational efficiency, making it a vital tool in the fight against cybersecurity threats.

TABLE II. COMPARISON OF TRADITIONAL AND PHYSICAL LAYER AUTHENTICATION

	Traditional Authentication	Physical Layer Authentication
Security Basis	Relies on cryptographic algorithms such as RSA and AES. Security depends on key secrecy.	Exploits unique wireless channel properties like CSI and RSSI, making authentication independent of cryptographic keys.
Quantum Resistance	Vulnerable to quantum attacks due to reliance on cryptographic keys. Post-quantum cryptography is required for future security.	Resistant to quantum attacks since authentication relies on unpredictable physical-layer characteristics rather than computationally hard problems.
Resource Requirement	High, requiring significant computational power for key generation, encryption, and decryption, making it unsuitable for low-power IoT devices.	Moderate, well-suited for resource-constrained IoT and edge devices as it leverages inherent wireless properties, eliminating heavy cryptographic processing.
Scalability	Limited in large-scale networks due to complex key management overhead and reliance on centralized authentication infrastructures.	Highly scalable as it does not require pre-shared keys; authentication can be conducted dynamically based on wireless channel variations.
Adaptability to Mobility	Performs poorly in dynamic environments such as vehicular networks due to frequent key exchanges and high latency.	Naturally adapts to mobility as authentication is based on real-time variations in wireless channel characteristics, ensuring robust security in mobile environments.
Implementation Complexity	Requires digital certificates, complex key distribution protocols, and secure storage for cryptographic keys, increasing management overhead.	Lower complexity as it leverages existing wireless channel characteristics without requiring additional cryptographic infrastructure.
Real-World Use Cases	Post-Quantum Security: 5G/6G networks require new cryptographic schemes to counter quantum threats. Traditional key-based authentication in IoT devices suffers from high computational overhead, vulnerability to channel fluctuations, and reconciliation overhead.	5G/6G Authentication: environment semantics enabled physical layer authentication network based on deep learning enhances security against physical layer spoofing attack in next-generation networks [12]. Lightweight, continuous authentication scheme utilizing IoT transmission model properties significantly reduces misdetection rates and computational costs [13].

B. Blockchain-Based Authentication

The proliferation of Internet of Things (IoT) devices and distributed networks has necessitated the development of robust, decentralized authentication mechanisms to ensure security and privacy. Traditional centralized authentication systems often become bottlenecks and single points of failure, making decentralized approaches more appealing for scalable and resilient IoT ecosystems.

Decentralized Authentication Mechanisms: Recent advancements have leveraged blockchain technology and Decentralized Identifiers (DIDs) to create trustless authentication systems. For instance, the integration of blockchain in IoT services has been proposed to enhance security, data integrity, user privacy, system scalability, and device interoperability. This approach utilizes smart contracts to enforce authentication, access control, and data exchange mechanisms among IoT devices [19].

Case Studies: A notable implementation is the DAXiot scheme, which employs DIDs and Verifiable Credentials for decentralized authentication and authorization in dynamic IoT networks. This privacy-preserving challenge-response mechanism facilitates decentralized permission management and supports authenticated encryption for data confidentiality. Demonstrations in Message Queuing Telemetry Transport (MQTT) 5.0 scenarios have validated its security, privacy guarantees, and performance [20].

Another study introduced a blockchain-based decentralized identity system tailored for IoT networks, focusing on a novel serialization mechanism for DID documents and a binary message envelope for secure communication. This design addresses the practical challenges of implementing Self-Sovereign Identity (SSI) in constrained IoT environments, significantly reducing the size of identity metadata and security overhead [21].

Implementation Challenges: Despite these advancements, several challenges persist in deploying decentralized authentication in IoT and distributed networks:

- Resource Constraints: IoT devices often have limited computational power and storage, making the implementation of resource-intensive blockchain solutions challenging. Lightweight protocols and efficient cryptographic algorithms are essential to mitigate this issue.
- Scalability: As the number of IoT devices increases, maintaining a decentralized authentication system that can scale efficiently without compromising performance or security is critical.
- Interoperability: Ensuring seamless interaction between heterogeneous devices and systems requires standardized protocols and frameworks.
- Latency: Real-time applications demand low-latency authentication processes, which can be hindered by the inherent processing times of blockchain transactions.

Addressing these challenges involves ongoing research into optimizing decentralized authentication protocols, developing lightweight cryptographic methods, and creating scalable blockchain architectures tailored for IoT environments.

C. Quantum-Resilient Authentication

The advent of quantum computing poses significant challenges to current cryptographic systems, necessitating the transition to post-quantum cryptography (PQC) to safeguard data against future quantum attacks. Recent developments have focused on preparing for PQC and its seamless integration into existing network infrastructures. Preparing for Post-Quantum Cryptography: The National Institute of Standards and Technology (NIST) has been at the forefront of standardizing PQC algorithms. Recently, NIST released three finalized algorithms designed to

withstand quantum attacks, marking a pivotal step toward quantum-resistant security solutions. These algorithms are expected to be adopted by federal agencies and the private sector to ensure long-term data security [22].

Integration with Existing Network Infrastructures: Integrating PQC into current network systems presents several challenges, including compatibility with existing protocols, computational efficiency, and minimal disruption to services. A study by Hoque et al. proposed a quantum-secure architecture combining PQC and Quantum Key Distribution (QKD) tailored for sustainable mobile networks. This architecture addresses the complexities of protecting critical infrastructures against future quantum attacks while considering operational sustainability [23].

Additionally, Kempf et al. demonstrated the feasibility of integrating post-quantum cryptographic algorithms into the QUIC protocol, a modern transport layer network protocol. Their research highlights the potential for updating existing protocols to incorporate PQC without significant performance degradation [24].

Implementation Challenges: Transitioning to PQC involves addressing several implementation challenges:

- Performance Overhead: PQC algorithms may introduce increased computational requirements, potentially affecting network performance. Optimizing these algorithms for efficiency is crucial for their practical deployment.
- Standardization and Interoperability: Ensuring that PQC solutions are standardized and interoperable across diverse systems is essential for widespread adoption. Collaborative efforts among industry stakeholders are necessary to achieve this goal.
- Scalability: Implementing PQC in large-scale networks requires scalable solutions that can handle the increased complexity without compromising security or performance.

Addressing these challenges is imperative for the successful integration of PQC into existing network infrastructures, ensuring resilience against the emerging threats posed by quantum computing. Table III highlights emerging research in authentication technologies, focusing on hybrid authentication models, privacy-preserving techniques, and AI-augmented PLS, along with their key contributions.

TABLE III. EMERGING RESEARCH IN AUTHENTICATION TECHNOLOGIES

Research Focus	Key Contributions
Hybrid authentication models	Combination of biometrics and device-based credentials for enhanced robustness [32].
Privacy-preserving authentication	Use of homomorphic encryption to protect sensitive data during authentication [33].
AI-augmented PLS	Adaptive anomaly detection and dynamic authentication leveraging AI/ML models [35].

IV. AUTHENTICATION IN SPECIALIZED NETWORK ENVIRONMENTS

The increasing diversity and complexity of network environments demand authentication mechanisms tailored to specific use cases and challenges. From wireless networks with dynamic topologies to resource-constrained IoT devices and innovative technologies like VLC, the requirements for secure, efficient, and scalable authentication are continually evolving. This section examines specialized authentication schemes designed for unique environments, focusing on leveraging physical properties, adaptive protocols, and lightweight solutions. By exploring these approaches, we aim to provide insights into how these mechanisms address distinct challenges and enable secure communication across diverse and specialized network applications.

A. Wireless Networks

The integration of Multiple Input Multiple Output (MIMO) technology with cooperative relaying has proven to be a transformative approach to enhancing authentication mechanisms for wireless communication systems. These technologies, when combined, not only improve data throughput and reliability but also enable the creation of robust authentication frameworks that leverage spatial diversity and redundancy. This is particularly beneficial in mitigating eavesdropping and ensuring secure communication, especially in dynamic network scenarios.

MIMO systems utilize multiple antennas at both the transmitter and receiver, creating unique channel characteristics that are inherently resistant to spoofing and interception. Cooperative relaying further strengthens these mechanisms by incorporating intermediate relay nodes to forward messages securely. For example, recent research by Su et al. introduced a secure massive MIMO system utilizing two-way relay cooperative transmission. This system employs a multi-relay configuration, where some relays serve as helpers and others as jammers, effectively countering eavesdropping attempts and ensuring the security of 6G network communications [25].

Despite these advancements, several challenges persist in deploying MIMO and cooperative relaying for authentication. The integration of these technologies introduces additional complexity and computational overhead, which can impact real-time performance. Synchronization among multiple antennas and relays is another critical issue, particularly in fast-changing environments where precise timing is essential. Moreover, resource allocation among relay nodes, such as power and bandwidth, requires sophisticated optimization techniques to balance security and efficiency effectively.

Future research must focus on addressing these challenges through the development of scalable and adaptive algorithms. Machine learning techniques hold promise in optimizing resource management and enhancing the adaptability of authentication protocols. Lightweight cryptographic protocols that complement the physical-layer security advantages of MIMO and cooperative relaying are also crucial for achieving secure and efficient authentication in next-generation wireless networks.

B. Visible Light Communication

VLC leverages the visible spectrum to transmit data, offering unique physical characteristics that can be

harnessed to strengthen authentication mechanisms. The inherent line-of-sight nature and spatial confinement of VLC signals provide a foundation for developing robust security protocols.

Recent studies have explored the utilization of hardware imperfections in VLC devices to create distinctive identifiers, enhancing authentication processes. For instance, Chen *et al.* [28] introduced the concept of an "Optic Fingerprint," which capitalizes on the intrinsic circuit characteristics of Light Emitting Diodes (LEDs) to extract unique feature vectors. Their experimental evaluations demonstrated an impressive identification accuracy of up to 99.3% under varying conditions, highlighting the potential of this approach in bolstering physical layer security in VLC networks [26]. Additionally, advancements in material science have contributed to the development of novel security solutions in VLC systems. Han *et al.* [27] investigated the incorporation of gold nanoparticles with chiroptical properties into VLC setups. By introducing controlled phase retardation effects, these nanoparticles interact with linear polarizers to enhance the secrecy rate of communications. Their findings indicate that this method effectively mitigates eavesdropping risks, even when adversaries are in close proximity to legitimate receivers [27].

The potential applications of these findings are vast, ranging from secure indoor wireless networks to authentication in vehicular communication systems. By harnessing the unique physical properties of VLC, it is possible to develop authentication mechanisms that are not only secure but also efficient and cost-effective. However, challenges remain in standardizing these approaches and ensuring their scalability across diverse deployment scenarios. Table IV summarizes the unique physical properties of Visible Light Communication (VLC) and their applications, highlighting security benefits, optic fingerprinting, and secrecy enhancements through nanomaterials.

TABLE IV. UNIQUE PHYSICAL PROPERTIES AND APPLICATIONS OF VLC

Physical Property	Impact and Applications
Line-of-sight nature	Reduces signal propagation beyond physical boundaries, enhancing security in indoor wireless networks.
Hardware imperfections in LEDs	Enables "Optic Fingerprint" identification with 99.3% accuracy, as demonstrated [26].
Integration of nanomaterials	Enhances secrecy rate by leveraging chiroptical properties [27].

C. IoT and 6G Networks

The rapid expansion of the Internet of Things (IoT) has introduced significant challenges in authenticating a vast number of low-power, high-density devices. Traditional authentication mechanisms often fall short due to the constrained resources of these devices and the sheer scale of deployments. Recent research has focused on developing scalable and lightweight authentication protocols tailored to these specific requirements. Fig. 3 illustrates the layered approach, integrating device-level authentication with edge AI and cloud analytics while addressing common threats.

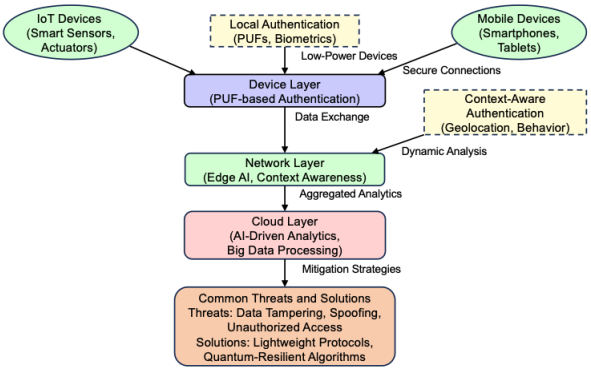

Fig. 3. Authentication architecture in IoT and 6G networks.

One of the primary challenges is the limited computational and energy resources inherent to IoT devices. Conventional cryptographic methods can be too resource-intensive, leading to increased latency and power consumption. To address this, lightweight cryptographic primitives have been proposed. For instance, Ahmed and Mohammed [28] conducted a comprehensive survey of lightweight authentication methods suitable for IoT environments, highlighting the need for identity management and authorization mechanisms that are both secure and resource-efficient.

Another significant challenge is the scalability of authentication protocols in high-density IoT deployments. As the number of connected devices increases, the authentication system must efficiently manage a vast number of entities without compromising performance. In this context, Physical Unclonable Functions (PUFs) have emerged as a promising solution. PUFs leverage inherent hardware variations to generate unique identifiers for devices, enabling secure and efficient authentication. Zhang and Li [29] proposed a lightweight PUF-based authentication protocol that addresses both security and scalability concerns in IoT applications.

Furthermore, the integration of Artificial Intelligence (AI) and Machine Learning (ML) techniques has been explored to enhance authentication processes. These technologies can adapt to dynamic network conditions and detect anomalies, thereby improving security. However, implementing AI/ML solutions in low-power IoT devices presents its own set of challenges, including the need for energy-efficient algorithms and hardware. Schizas *et al.* [30] discussed the role of TinyML—machine learning models optimized for resource-constrained devices—in enabling ultra-low-power AI for large-scale IoT deployments.

In conclusion, addressing the challenges of low-power, high-density IoT device authentication requires a multifaceted approach that combines lightweight cryptographic techniques, scalable protocols, and intelligent adaptive systems. Ongoing research continues to develop innovative solutions to meet the evolving demands of massive IoT deployments.

V. Challenges and Future Directions

The rapid expansion of large-scale networks has introduced significant challenges in authentication mechanisms, particularly concerning scalability and complexity. Traditional authentication systems often struggle to efficiently manage the vast number of devices and users in such environments, leading to increased latency and potential security vulnerabilities. Recent studies have highlighted the need for scalable and lightweight authentication protocols to address these issues effectively. For instance, Mao *et al.* [31] discussed the critical problems and security demands in large-scale network identity authentication, emphasizing the importance of selecting appropriate and effective authentication technologies for different scenarios to enhance security.

In biometric and Physical Layer Security (PLS)-based schemes, user privacy concerns remain paramount. The storage and processing of sensitive biometric data pose risks related to unauthorized access and potential misuse. To mitigate these concerns, researchers have proposed integrating advanced cryptographic techniques and decentralized storage solutions. For example, a blockchain-based biometric identity management system has been suggested to enhance security and privacy by eliminating the need for a centralized authority, thereby reducing the risk of data breaches [32].

Emerging research areas are exploring the convergence of Artificial Intelligence (AI) with PLS to develop AI-augmented PLS systems. These systems aim to enhance authentication by leveraging AI's ability to detect anomalies and adapt to dynamic network conditions. Additionally, hybrid authentication models that combine multiple authentication factors, such as biometrics and device-based credentials, are being investigated to provide more robust security frameworks. A recent study introduces Blind-Touch, a machine learning-based fingerprint authentication system that utilizes homomorphic encryption to address privacy concerns, demonstrating high accuracy and efficiency in privacy-preserving fingerprint authentication [33]. Fig. 4 and Table V highlight core challenges such as scalability and privacy, link them to corresponding solutions, and introduce research directions, including AI-augmented PLS and hybrid models [34, 35].

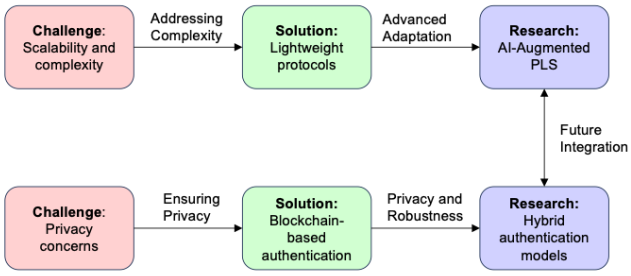

Fig. 4. Challenges, solutions, and emerging research directions in authentication mechanisms.

In dynamic and resource-constrained environments such as the IoT and vehicular networks, authentication mechanisms must balance security and efficiency. Traditional cryptographic methods, while providing robust security, often entail significant computational overhead, making them less suitable for devices with limited resources [36]. Conversely, physical-layer authentication leverages inherent properties of the communication medium, offering a lightweight alternative. However, this approach may face challenges related to channel variability and environmental factors, potentially affecting its reliability. Therefore, selecting an appropriate authentication scheme necessitates a careful assessment of the specific security requirements and operational constraints of the application scenario.

TABLE V. Summary of Challenges and Proposed Solutions in Authentication Mechanisms

Challenges	Proposed Solutions
Scalability and complexity in large-scale networks	Development of scalable, lightweight authentication protocols tailored for massive deployments [31].
User privacy concerns in biometric and PLS-based schemes	Integration of blockchain for decentralized storage and the use of homomorphic encryption to secure sensitive data, highlighted in blockchain-based biometric systems [32] and Blind-Touch models [33].
Hybrid authentication models	Combination of biometrics and device-based credentials for enhanced robustness, as seen in hybrid models leveraging multi-factor approaches [34].
Emerging research in AI-augmented PLS	Utilizing AI for anomaly detection and adaptive authentication in dynamic networks [35].

VI. Conclusion

This study reviewed authentication mechanisms designed for specialized network environments, highlighting their adaptability and efficacy in addressing complex challenges. The integration of MIMO and cooperative relaying technologies in wireless networks demonstrated substantial progress in mitigating eavesdropping risks and ensuring secure communication, particularly in high-mobility scenarios such as vehicular networks and high-speed trains. VLC emerged as a promising field, leveraging unique physical-layer properties like line-of-sight constraints and hardware imperfections to develop novel authentication techniques, including the "Optic Fingerprint." In the IoT and 6G domains, scalable and lightweight protocols, supported by advancements in Physical Unclonable Functions (PUFs) and TinyML, have shown great potential in addressing the constraints of high-density, resource-constrained environments.

The findings underscore the critical importance of interdisciplinary approaches that integrate physical-layer security, advanced cryptographic frameworks, and machine learning-driven adaptability. These approaches enhance the robustness, scalability, and efficiency of authentication mechanisms, ensuring their effectiveness in increasingly heterogeneous and dynamic network environments.

Looking ahead, the future of authentication in network security will depend on advancements in quantum-resistant algorithms, adaptive systems powered by

artificial intelligence, and sustainable, resource-efficient solutions. The interplay between cryptographic innovation, material science, and AI promises to reshape authentication paradigms, delivering solutions that are secure, scalable, and tailored to the demands of next-generation technologies and global connectivity. Collaborative research efforts and standardized frameworks across disciplines will be vital in driving these innovations and realizing the full potential of authentication systems in safeguarding the modern digital ecosystem.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] M. Azrour, J. Mabrouki, A. Guezzaz, and Y. Farhaoui, "New enhanced authentication protocol for internet of things," *Big Data Mining and Analytics*, vol. 4, no. 1, 2021.

[2] I. Radhakrishnan, "security evaluation of lightweight cryptographic algorithms for resource-constrained IoT devices," *Sensors*, vol. 24, 2024.

[3] M. A. Arfaoui *et al*., "Physical layer security for visible light communication systems: A survey," *IEEE Communications Surveys and Tutorials*, vol. 22, pp. 1887–1908, 2020.

[4] J. Cook, S. U. Rehman, and M. A. Khan, "Security and privacy for low power IoT devices on 5G and beyond networks: Challenges and future directions," *IEEE Access*, vol. 11, pp. 39295–39317, 2023.

[5] A. N. Alsheavi *et al*., "IoT authentication protocols: Classification, trend and opportunities," *IEEE Transactions on Sustainable Computing*, no. 1, pp. 1–20, 2024.

[6] M. Rana, Q. Mamun, and R. Islam, "Current lightweight cryptography protocols in smart city IoT networks: A survey," arXiv preprint arXiv:2010.00852, 2020.

[7] R. Bavdekar *et al*., "Post quantum cryptography: Techniques, challenges, standardization, and directions for future research," arXiv:2202.02826, 2022.

[8] M. S. Henriques and N. K. Vernekar, "Using symmetric and asymmetric cryptography to secure communication between devices in IoT," in *Proc. 2017 International Conference on IoT and Application (ICIOT)*, Nagapattinam, 2017, pp. 1–4.

[9] H. Fang, X. Wang, and L. Hanzo, "Learning-aided physical layer authentication as an intelligent process," *IEEE Transactions on Communication*, vol. 67, pp. 2260–2273, 2019.

[10] Q. Wang *et al.*, "Supervised and semi-supervised deep neural networks for CSI-based authentication," arXiv preprint arXiv:1807.09469, 2018.

[11] X. Lu *et al.*, "Analytical method of physical layer authentication for performance evaluation," *IEEE Globecom Workshops (GC Wkshps)*, Rio de Janeiro, Brazil, pp. 257–262, 2022.

[12] N. Gao *et al.*, "EsaNet: Environment semantics enabled physical layer authentication," *IEEE Wireless Communications Letters*, vol. 13, pp. 178–182, 2024.

[13] S. Khan, C. Thapa, S. Durrani, and S. Camtepe, "Access-based lightweight physical-layer authentication for the internet of things devices," *IEEE Internet of Things Journal*, vol. 11, pp. 11312–11326, 2024.

[14] T. N. Ha and D. Romero, "Spoofing detection in the physical layer with graph neural networks," in *Proc. 2024 IEEE 99th Vehicular Technology Conference*, vol. 11, no. 2, 2024.

[15] P. Schummer *et al.*, "Machine learning-based network anomaly detection: Design, implementation, and evaluation," *Artificial Intelligence for Network Management*, vol. 5, pp. 2967–2983, 2024.

[16] G. Wei and Z. Wang, "Adoption and realization of deep learning in network traffic anomaly detection device design," *Soft Computing*, vol. 25, pp. 1147–1158, 2021.

[17] M. Hazratifard, F. Gebali, and M. Mamun, "Using machine learning for dynamic authentication in telehealth: A tutorial," *Sensors*, vol. 22, 7655, 2022.

[18] A. Karras *et al*., "TinyML algorithms for big data management in large-scale IoT systems," *Future Internet*, vol. 16, no. 42, 2024.

[19] A. Perrusquía *et al*., "A novel distributed authentication of blockchain technology integration in IoT services," *IEEE Access*, vol. 12, pp. 12345–12356, 2024.

[20] A. Philipp and A. Küpper, "DAXiot: A decentralized authentication and authorization scheme for dynamic IoT networks," arXiv preprint arXiv:2307.06919, 2023.

[21] G. Fedrecheski *et al*., "A low-overhead approach for self-sovereign identity in IoT," *Global IoT Summit*, pp. 265–276, 2021.

[22] UNIST Releases First 3 Finalized Post-Quantum Encryption Standards. National Institute of Standards and Technology (NIST). [Online]. Available: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[23] S. Hoque, A. Aydeger, and E. Zeydan, "Exploring post quantum cryptography with quantum key distribution for sustainable mobile network architecture design," in *Proc. 4th Workshop on Performance and Energy Efficiency in Concurrent and Distributed Systems*, 2024, pp. 9–16.

[24] M. Kempf *et al*., "A quantum of QUIC: Dissecting cryptography with post-quantum insights," in *Proc. 2024 IFIP Networking Conference (IFIP Networking)*, 2024, p. 1.

[25] Y. Su *et al*., "Secure massive MIMO system with two-way relay cooperative transmission in 6G networks," *EURASIP Journal on Wireless Communications and Networking*, no. 73, 2023.

[26] X. Chen *et al*., "Optic fingerprint: Enhancing security in visible light communication networks," in *Proc. IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2024.

[27] G. Han *et al*., "On the physical layer security of visible light communications empowered by gold nanoparticles," *Journal of Optical Communications and Networking*, vol. 16, no. 7, pp. 750–763, 2022.

[28] W. K. Ahmed and R. S. Mohammed, "Lightweight authentication methods in IoT: Survey," in *Proc. International Conference on Computer Science and Software Engineering (CSASE)*, 2022, p. 1.

[29] Y. Zhuang and G. Li, "A lightweight PUF-based authentication protocol," arXiv preprint arXiv:2405.13146, 2024.

[30] N. Schizas *et al*., "TinyML for ultra-low power AI and large scale IoT deployments: A systematic review," *Future Internet*, vol. 14, no. 12, p. 363, 2022.

[31] R. Mao *et al*., "Discussion on key technologies of identity authentication in large-scale networks," *Journal of Cyber Security*, 2023.

[32] S. H. G. Salem *et al*., "Blockchain-based biometric identity management," *Cluster Computing*, vol. 27, pp. 3741–3752, 2024.

[33] H. Choi *et al*., "Blind-Touch: Homomorphic encryption-based distributed neural network inference for privacy-preserving fingerprint authentication," in *Proc. AAAI Conference on Artificial Intelligence*, vol. 38, no. 20, 2023.

[34] S. K. Choudhar and A. K. Naik, "Multimodal Biometric authentication with two-layer hybrid template security," *SN Computer Science*, vol. 5, no. 785, 2024.

[35] C. Y. Zhao *et al*., "Generative AI for secure physical layer communications: A Survey," *IEEE Transactions on Cognitive Communications and Networking*, vol. 11, no. 1, 2024.

[36] L. Bai *et al*., "Physical layer authentication in wireless communication networks: A survey," *Journal of Communications and Information Networks*, vol. 5, pp. 237–264, 2020.