Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Review of the Evaluating Authentication Approaches for Emerging Risks and Chaotic Systems in 5G Network Security

Israa J. Mohammed Al-Kalfa[1,2 *], Jorge Munilla[1], Karam J. Mohammed[3], Mohammed Harbi Adhab[4], Abdulmajeed Al-Jumaily[5]

[1] *Department of Telecommunication Engineering, Malaga University, Malaga, Spain.*
Email: Israa_jassim2011@uma.es, Munilla@ic.uma.es
[2] *Information Technology and Communication Research Center, Ministry of Higher Education & Scientific Research, Baghdad, Iraq.*
Email: Israa.j.mohammed@src.edu.iq
[3] *Space Research and Technology Center, Ministry of Higher Education & Scientific Research, Baghdad, Iraq.*
Email: drkaramjasim@gmail.com
[4] *Scientific Research Commission, Ministry of Higher Education & Scientific Research Baghdad, Iraq. Email: mohammed.h.adhab@src.edu.iq*
[5] *Department of Signal Theory and Communications (DTSC), Charles III University of Madrid, UC3M, Leganes, Spain.*
Email: abdulmajeed@tsc.uc3m.es
** Corresponding Author: Israa J. Mohammed Al-Kalfa, E-mail: Israa_jassim2011@uma.es, israa.j.mohammed@src.edu.iq*

ARTICLE INFO

Received:01 Jul 2025

Revised:05 Aug 2025

Accepted: 15 Aug 2025

ABSTRACT

With previously unheard-of improvements in connection, latency reduction, and data transfer rates, 5G technology users are in a new age in mobile communications. From augmented reality and driverless cars to industrial automation and the Internet of Things (IoT), these capabilities have sparked a variety of applications. Making sure 5G networks are secured has become crucial as they become a part of vital infrastructures. The foundation for building trust between devices, people, and networks is authentication, which stands out among the other security features. The authentication mechanisms designed for 5G applications are examined in this review, focusing on how they let users, devices, and network infrastructure communicate securely. Additionally, it examines the evolving threat landscape, including impersonation, replay attacks, man-in-the-middle (MitM) attacks, and signaling storms, that target authentication.

Keywords: 5G technology, Chaotic systems, Mobile communications, Authentication mechanisms, Security features, IoT.

INTRODUCTION

With promises of unprecedented innovation in connectivity, speed, and efficiency, 5G networks represent a revolution in communications technology. 5G is the cornerstone of new innovative applications like telemedicine, smart cities, industrial automation, augmented reality, and autonomous vehicles. 5G can potentially connect billions of devices in real-time seamlessly. However, there are serious security risks associated with 5G. Therefore, robust authentication mechanisms are required to enable the secure operation of ecosystems supported by this shift and prohibit unauthorized usage by allowing only verified users and devices to connect to the network. Authentication is the first line of defense in 5G networks (Al-Jumaily, Sali, et al., 2023), where only legitimate individuals, devices, and businesses are permitted. As 5G enables mission-critical services, failure of authentication mechanisms results in catastrophic consequences ranging from data breaches to service disruption and physical damage in use cases like healthcare and autonomous transportation. Authentication is the first line of protection.

One of the key protocols ensuring secure communication in 5G networks is the 5G Authentication and Key Agreement (5G AKA) protocol. This protocol enhances security by providing mutual authentication between users and the network while also establishing encryption keys for secure data transmission. This article also investigates more recent methods like as blockchain (Hojjati, Shafieinejad, & Yanikomeroglu, 2020). AI-based anomaly detection, and quantum-resistant encryption that improve authentication and reduce attack surfaces to ensure secure communication between users, devices, and network infrastructure. They discuss the most recent challenges to

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

authentication, including impersonation, signaling storms, replay attacks, and man-in-the-middle (MitM) assaults (Cekerevac, Cekerevac, Prigoda, & Al-Naima, 2025). **The main key contributions of this article are as follows:**

- **Chaotic Systems in Authentication**

The integration of chaotic structures into authentication processes is investigated as a unique way to improve security in 5G networks. The research explores how chaotic structures can be employed for dynamic key areas and stable discourse, particularly in aid-constrained scenarios (Gil Jiménez, Al-Jumaily, Sali, & Al-Jumeily, 2023).

- **Comprehensive Analysis of 5G Authentication**

The study provides a complete review of authentication systems in 5G networks that specialize in ensuring communication between users, devices, and infrastructure, while also addressing emerging risks such as impersonation, and replay attacks.

- **Integration of Advanced Technologies**

It investigates novel solutions such as blockchain, AI-driven anomaly detection, quantum-resistant encryption, and chaotic systems for dynamic key technology, which provide improved security and adaptability for 5G networks.

- **Lightweight solutions for IoT and resource-constrained devices**

The examination focuses on scalable and efficient authentication systems designed for IoT devices and coffee-powered environments, balancing security with minimal computational and statement operations complexity.

- **Real-time Threat Mitigation and Privacy Enhancements**

The research focuses on real-time threat detection, adaptive authentication, and privacy-preserving solutions such as Variable Radio Network Temporary Identifier (V-RNTI) to increase user anonymity and security in 5G networks.

- **Future directions and research gaps.**

Key research, gaps, and future instructions for 5G authentication are identified. Further investigation of quantum-secure protocols, AI-driven security applications, distributed authentication scenarios, and chaotic systems are being advocated and intended for providing a framework for future research in this domain.

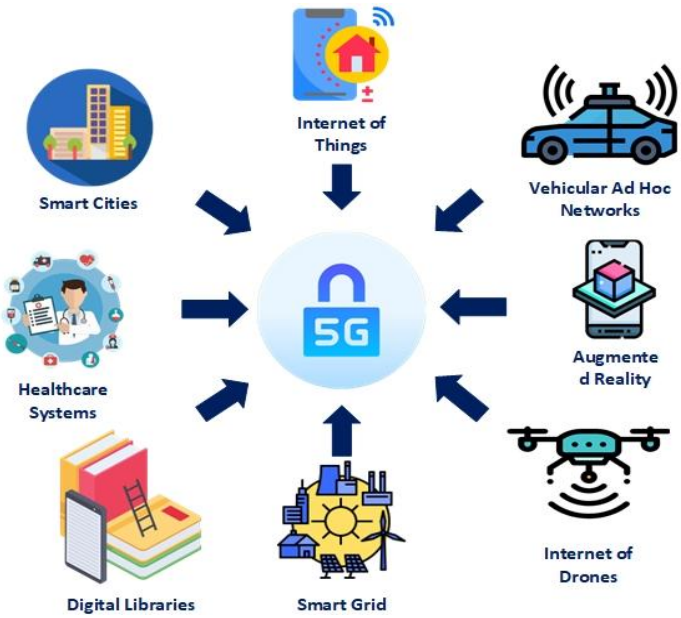

Figure 1: 5G authentication security applications overview.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

RESEARCH BACKGROUND

A. 5G Network

The 5G Core (5GC) is the foundation of 5G networks, designed with a flexible and secure cloud-native architecture. It ensures identity protection (SUCI), data encryption, and secure API communication while supporting applications like eMBB and URLLC. Key functions such as AMF (mobility management), SMF (session management), UPF (data handling), and NSSF (network slicing) enhance network performance. See figure (1) and table 1.

Figure 2: Components of 5G core network.

For secure packet transmission in 5G/B5G/6G networks, encrypting data at the source and decrypting it at the destination. It uses symmetric or asymmetric encryption based on security needs and adds protection against replay and manipulation with timestamps and message authentication codes (Al-Jumaily, Alrubaee, et al., 2023). The author proposed a Group Key utilizing Initial Key Agreement (GKIKA) architecture that encrypts packets at the source edge computer (EC) and decrypts them at the destination ECs (Hsiao et al., 2024). Addressing data leakage and replay risks proposed a 5G architecture using cryptography timestamp and message authentication codes. By using Deep Learning to optimize static and dynamic key generation to balance security and transmission delay between User Plane Functions (UPFs) (Susanto & Leu, 2022). An Elliptic Curve Cryptography (ECC) based multi-factor 5G-AKA authentication protocol was proposed by (Yadav et al., 2022), to improve security and efficiency.

It guarantees strong authentication for 5G networks while cutting costs by more than 50% in computing, communication, storage, and energy. To address the shortcomings of the 5G AKA protocol, including SUCI replay attacks, a lack of mutual authentication, and compromised location privacy suggested by (Y. Xiao & Wu, 2022). The 5G-IPAKA protocol. This protocol's improvements include mutual authentication, challenge-response techniques, derivation keys, and a timeout mechanism to prevent Message Authentication Code (MAC) failure exploitation.

Security and privacy by proposing a quantum-safe Authentication and Key Agreement protocol for 6G networks proposed by (Damir, Meskanen, Ramezanian, & Niemi, 2022). The protocol ensures full forward secrecy and key verification between the user equipment (UE) and serving network (SN) by leveraging post-quantum cryptography to improve security and privacy. It is computationally efficient and resilient to desynchronization, link-ability, and denial-of-service assaults. The topic of location privacy in 5G mobile communications is covered by (Saeed et al., 2022). By permitting frequent changes in pseudonyms, the suggested solution's innovative Variable Radio Network Temporary Identifier (V-RNTI) algorithm enhances user privacy by making tracking more challenging. With very few adjustments, this strategy can be included in the current 3GPP design. ProVerif Model Checker was used to validate the suggested V-RNTI-based authentication protocol, showing that it is compatible with earlier mobile network standards effectively preserving anonymity and hindering attackers from identifying users.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Classic security protocols are insufficient for modern requirements like lightweight and real-time communication. To address these issues, the authors (Mahmood et al., 2022), proposed a lightweight authentication scheme for Mobile Edge Computing (MEC). It supports mobile users' privacy and forward/ backward secrecy. And defense against threats like session key compromise and impersonation. Confirmed by both formal and informal security models. Location Services Authentication and Key Agreement (LS-AKA) was proposed by (Gupta, Pradhan, Chaudhari, & Singh, 2023), to address security issues with 5G-AKA, such as signaling congestion, absence of key forward/backward secrecy (KFS/KBS) techniques, and lack of key secrecy, LS-AKA uses group-leader approach and incremental hashing for efficient administration, ensuring mutual authentication, integrity, and anonymity. It offers reduced overhead and enhanced privacy, as confirmed by the Random Oracle Model (ROM).

Introduced the Authentication and Key Agreement-Forward Security (5G-AKA-FS) protocol to address weaknesses like UE unlikability and lack of forward secrecy in 5G-AKA. By using an ephemeral key pair for session key negotiation proposed by (You et al., 2023), the protocol ensures a robust forward. The security is validated using BAN Logic and Pro Verify, and it remains compatible with existing 5G-AKA systems with minor upgrades by (Ananthula & Budde, 2023), proposed to overcome security concerns with smart healthcare systems by leveraging 5G security standards. Lowering these possible risks by utilizing robust insufficient gains in data security and priority is demonstrated by the suggested solution. According to the results, 5G security standards might successfully lower security risks in intelligent healthcare systems and create a secure and reliable platform for medical service delivery. In addition to supporting state-of-the-art medical equipment, this approach significantly improves patient data security and ensures better patient outcomes within a safe and efficient framework.

According to the results, encryption methods, including Advanced Encryption Standard (AES) in Counter with CBC-MAC (CCM) mode (AES-CCM) and Elliptic Curve Diffie-Hellman (ECDH), between 5G-AKA and smart medical devices. Focus on improving security in 5G networks by addressing impersonation, replay, and jamming threats. The protocol proposed a problem that has been tested using AVISPA tools and evaluated with Open-Source Finite Model Checking (OFMC) and Classical Attack on Session Encryption, (CL-At Se), which ensures safe handovers and mutual authentication while maximizing speed and reducing costs (Benfarhi, 2024). Examines user privacy in Mobile Virtual Network Operators (MVNOs) from pre-5G to 5G. A study by (Alnashwan et al., 2024).

They provide a privacy-focused authentication and handover method that simplifies safe validation between MVNOs and MNOs while ensuring user anonymity and unlikability. An important step forward in 6G security is the planned DMRN (Decentralized Multi-Round Negotiation Protocol) Protocol, which combines PQC and PFS while maintaining compatibility with 3GPP standards. Formal analysis, however, highlights the need for additional improvements by exposing weaknesses like replay and HN masquerade attack (You, Kim, Pawana, & Ko, 2024).

To increase security and efficiency, suggested by (Kumar, Kumar, Manoranjithem, & Gottumukkala, 2024), a 5G Secure Handover Protocol that makes use of fuzzy logic and spiking neural networks. It ensures forward secrecy, cuts down on handover time, and protects against different types of assaults. A stochastic framework to enhance 5G infrastructure resilience by focusing on high availability ("five nines" reliability) and performance optimization with minimal redundancy. Also Analyzed delays in 5G nodes (AMF, SMF, UPF) using non-product-form queuing networks to address node failures and rejuvenation with stochastic reward networks and reliability block diagrams tested on an Open5GS test bed, the framework provides insights into reducing delays, optimizing redundancy, and understanding rejuvenation effects (De Simone, Di Mauro, Natella, & Postiglione, 2024).

B. Internet of Things (IoT)

5G offers the Internet of Things (IoT) two advantages: faster speeds and wider connections. However, it also presents substantial security concerns for authentication. IoT devices require robust and efficient security mechanisms to ensure that only authorized users may connect to the network because they often have limited resources. The (5G-AKA) protocol and advanced encryption improve security while satisfying IoT-specific needs. However, there are still significant challenges with scalability, privacy, and lightweight solutions for small devices. See figure (2) See table 2.

A secure protocol for healthcare services that ensures data integrity, privacy, and attack resistance (resistances to replay, DoS, and stolen credentials) is offered by (Chander & Gopalakrishnan, 2022b), using Radio Frequency

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Identification (RFID) and Traffic Management Information System (TMIS). It addresses the complexity and flaws of existing systems, with security verified by programs like AVISPA and Scyther and BAN logic-based GNY logic. The lightweight, three-factor SIP-based authentication method for HC-IoT developed by (Chander & Gopalakrishnan, 2022a), is officially security-analyzed using the Real-Or-Random (ROR) model and employs an expanded fractional Chebyshev chaotic map (FCCM). This method is secure, and efficient, and reduces the cost of computers, storage, and communication. To solve security issues in intelligent healthcare systems.

Presents a strong single-user sign-in (S-USI) authentication technique for Cloud of Medical Things (CoMT) applications. The suggested S-USI mechanism offers improved security for telecare medical information systems (TMIS) by utilizing the Chebyshev chaotic-map and the decisional Diffie-Hellman problem (DDHP). Employs a unary-token approach to ensure protection against replay, denial-of-service attacks, and insider threats while preventing clock synchronization issues. The S-USI method is validated using formal verification approaches like BAN logic and AKE session-key security, which show how resistant it is to hostile assaults. Cloud-based sensor intelligence networks can benefit from comparative analysis's lower computing, communication, and storage overhead (Deebak & Al-Turjman, 2023).

The goal of this article is to improve the security of authentication methods for EV charging systems, which share sensitive user data including payment credentials and identification (Mookherji, Odelu, & Prasath, 2024). Under the (Mutlaq et al., 2024), pointing out flaws such as vulnerability to Man-in-the-Middle (MITM) attacks. Because of this adversary model, the protocol developed by Wang et al. is not appropriate for use in industrial settings the paper proposes an improved authentication protocol that provides robust security against all known attacks under the Canetti-Krawczyk (CK) adversary model to verify its efficacy, a comprehensive security study employing the Real-Or-Random (ROR) paradigm is carried out. Furthermore, the suggested protocol exhibits improved security and efficiency for industrial implementation as compared to current systems.

By addressing problems like electrical quality and reliability, the Internet of Things (IoT) enhances smart grid management and contributes to the development of smart cities. Since smart grids communicate via public channels, smart meters are vulnerable to both physical and cyber-attacks. A simple mutual authentication system, as a solution to various security issues, which include confidentiality, integrity, and authentication. The plan ensures safe communication between smart meters, home area networks, gateways, and service providers by preventing attacks with physical unclonable functions (PUFs). Security study demonstrates that the scheme is more resilient to attacks and performs more efficiently in computing and communication than current protocols (Hafeez, Shakib, & Munir, 2025; Khalaf & Mohammed, 2024).

A lightweight authentication method for the Internet of Things based on Physical Unclonable Functions (PUFs) and Chebyshev chaotic maps for two-way authentication and session key negotiation was proposed by (Jin et al., 2024). The method meets 12 security standards, including safeguarding user privacy, and is impervious to physical and machine learning attacks. Tools such as ProVerif and upgraded BAN logic are used for security verification. A lightweight AKA protocol for 5G-enabled IoT that ensures secure, low-latency handovers in edge-fog-cloud systems. By author (L. Zhang, Wu, Liu, Guan, & Yin, 2024) proposed, the use of AES encryption enhanced security reduces transmission costs by 30%, and enables fast authentication (0.243 ms). It is more efficient and appropriate for devices with limited resources than TLS 1.3 and 5G-AKA.

Edge computing and artificial intelligence (AI) can be integrated with IoT (EC-IoT) systems to address security and privacy issues in IoT networks, as proposed by (Rupanetti & Kaabouch, 2024). The focus is on AI-based approaches to threat identification and mitigation, and it looks at the latest developments, threat models, and their effects. It highlights the need for scalable and robust solutions to handle new EC-IoT concerns, classifies AI-driven security frameworks, and investigates the optimization of AI algorithms for edge-based systems. It also identifies open problems and suggests future lines of inquiry to enhance the security, privacy, and functionality of EC-IoT systems. The author (Thapliyal et al., 2024), suggested a SAIoT-SL which is a secure AIoT-enabled authenticated key agreement system designed to address energy waste and improve security in smart home settings. SAIoT-SL guarantees dependable connection between cloud servers, users, and sensors. This has been confirmed by comparison analysis using the Scyther tool.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Figure 3: Components of SAIoT-SL system.

C. Internet of Drone

The Internet of Drones (IoD) and 5G technology work together to offer ultra-low latency, high-speed connections, and massive device capacity. These developments allow drones to perform complex tasks like autonomous navigation, real-time video streaming, and swarm coordination. 5G also introduces strong authentication mechanisms, such as the 5G Authentication and Key Agreement (5G-AKA) protocol, which provides enhanced mutual authentication and encryption to prevent cyber-attacks and unauthorized access. However, there are still issues, such as scalability for large drone fleets and lightweight security solutions designed for drones with limited computational power. A lightweight AKA scheme for secure drone-user communication on the Internet of Drones (IoD), supported by a server, proposed by (Pu, Choo, & Korać, 2024).

A safe and effective drone identification system for smart cities that facilitates real-time data sharing through the Internet of Drones (IoD) and public engagement through mobile devices. The open communication environment and the sensitive nature of the shared data make it imperative to address privacy and security issues. The suggested technique takes advantage of elliptic curve cryptography (ECC) to get over drones' energy and processing constraints while maintaining user privacy, data secrecy, and attack defense. Formal validation and comparative studies have shown that it is more secure and effective than current options, making it a perfect fit for smart city mobility and surveillance (Shah et al., 2024).

LAKA-UAV, a safe architecture for cloud-assisted UAVs in Flying Ad-hoc Networks (FANETs), is proposed by (Yu, Lee, Sutrala, Das, & Park, 2023). Blockchain is being used by UAVs in FANETs to govern access and maintain data integrity. The ROR oracle model validates the session key security of the framework, while AVISPA simulations verify that it is resistant to replay and MITM attacks, guaranteeing effective and safe UAV-cloud communication. LAPEC Lightweight Authentication Protocol with Elliptic Curve, an ECC (Elliptic Curve Cryptography), based authentication protocol for UAVs, ensuring backward secrecy and improved flexibility. It minimizes overhead and aims for future optimization and UAV-to-UAV communication applications (S. Zhang, Liu, Han, & Yang, 2023).

Figure 4: Components of UAV security Strategies.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Most existing security systems are incompatible with UAV sensors. These protocols often do not address attacks such as side routing, de-synchronization, and session leakage presented a lightweight authentication protocol that uses hash functions and quadratic residues (Nyangaresi, Alsolami, & Ahmad, 2024). Its robustness is shown by formal analysis using the random oracle model and informal analysis under the Dolev-Yao and Canetti-Krawczyk threat models. The integration of satellite networks and Unmanned Aerial Vehicle (UAV) networks within the Space-Air-Ground 6G framework presents security problems, it draws attention to satellite networks caused by significant propagation delays and erratic connectivity, such as eavesdropping, manipulation, and impersonation. The study suggested a safe networking authentication method for satellite and UAV nodes that makes use of the Chebyshev polynomial and elliptic curve public key cryptography (Li, Cao, Shi, & Li, 2024).

D. Digital Library+

5G enhances digital libraries with real-time collaboration and fast access to multimedia content while ensuring secure authentication through protocols like 5G-AKA. However, challenges include scaling authentication for growing users, lightweight security for mobile devices, and maintaining data integrity in distributed systems. Overcoming these issues is crucial for secure and efficient 5G-powered digital libraries.

Chebyshev chaotic mapping-based security authentication technique for digital libraries that integrates biometric, smart card, and password factors to provide secure session key generation and strong user verification. It uses Physical Unclonable Function (PUF) technology to protect personal data. Security analysis and performance tests show that the approach ensures robust security and efficient authentication. To improve scalability and efficiency for scenarios involving high numbers of users, future research will focus on using distributed computing frameworks (W. Xiao, Liu, & Yin, 2024).

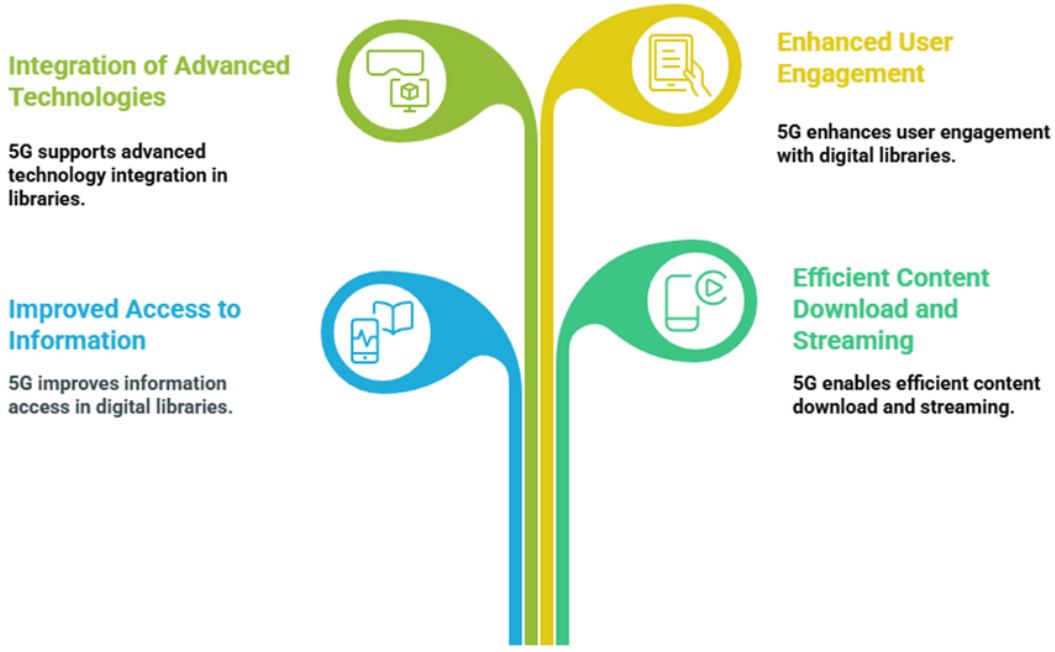

Figure 5: Enhancing digital libraries with 5G.

This blockchain technology points out for enhancing DRM in digital libraries to serve as a protective framework for licit intellectual property in view of unauthorized access, inefficient licensing, and lack of transparency. Building on foundational principles of blockchain, suggested a decentralized and tamper-proof ledger to manage digital rights within the library ecosystem and smart contracts to improve content security, streamline licensing, and reduce administrative burdens. Decentralized identity systems give users more control over personal data while maintaining security. It demonstrates the potential of blockchain, retaining accountability and redefining digital content distribution in safeguarding and optimizing digital libraries as safe and efficient repositories in the modern age (Tamilselvan, 2024).

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

E. Augmented reality (AR)

Augmented reality (AR) enables digital content overlay for training, meetings, gaming, and shopping. However, its immersive nature raises security risks, requiring trusted networks, devices, and users. For 5G-powered AR to be secure and reliable, strong authentication is essential. Key challenges include lightweight security for AR devices and privacy protection in real-time interactions.

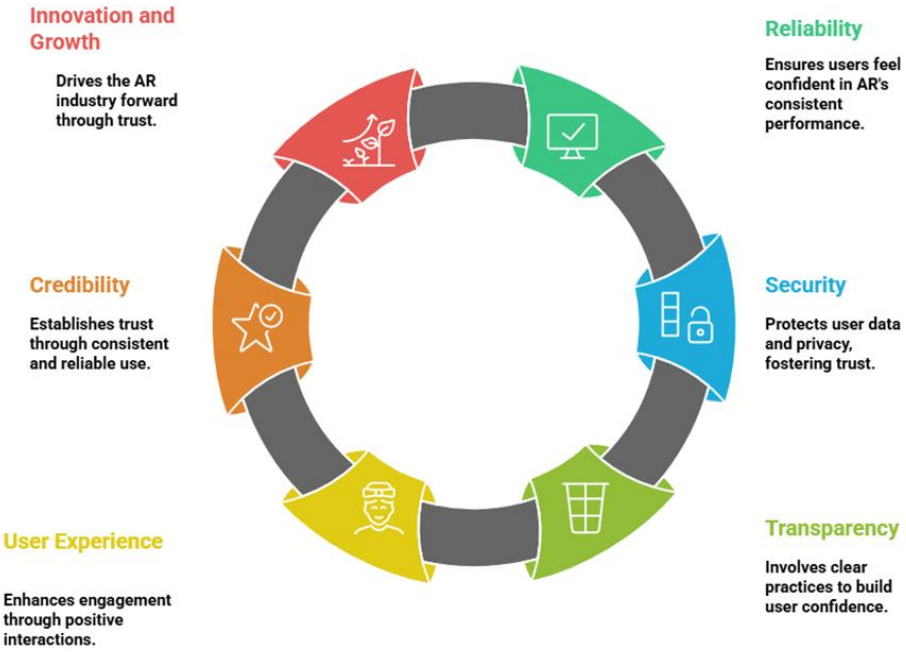

Figure 6: Building trust in AR.

Systems have transformative applications in industries like entertainment, healthcare, and education but introduce critical security and privacy challenges. These are some of the potential risks: input validation vulnerabilities, user tracking, data misuse, and manipulation of immersive feedback. AR and VR Systems Security, While current mitigation strategies, including robust authentication, data encryption, and conflict resolution frameworks, address some issues, significant gaps remain (Abid). The security issues surrounding the use of augmented reality (AR) in business settings, with particular attention on device vulnerabilities, network security, data privacy, and authentication. It offers a comprehensive framework with recommendations for safe implementation that considers technological, legal, ethical, and human-centric factors. The primary recommendations include policy creation, employee training, regular audits, adherence to the law, and device security. To safeguard enterprise data while using AR's potential (Hatami et al., 2024).

A secure and portable edge computing-based authentication method for augmented reality (AR) settings, found the protocol offers efficient security for user-to-user (U2U) and user-to-infrastructure (U2I) authentication by utilizing physical unclonable functions (PUFs) and Chebyshev chaotic maps. Session keys begin following U2I authentication to enable safe, real-time data flow between users. The security of the protocol is examined using tools like BAN logic, the Scyther tool, and the Real-Or-Random model, which demonstrate that it is resilient to a range of attacks (Kwon & Park, 2024).

Comparative investigation utilizing the Multi-precision Integer and Rational Arithmetic Cryptographic Library MIRACL cryptography SDK confirms its low computational and communication costs, which make it suitable for resource-constrained AR edge situations concentrated on elements including control flow graphs, permissions, API calls, and metadata using a dataset of 408 AR/VR apps from the Google Play Store. Over half of applications are vulnerable while delivering data, even if the majority don't include dangerous stuff. In recent years, AR/VR applications for entertainment and education have grown significantly in popularity, many of these programs support a broad age range and are cross-platform compatible, including standardized data modalities, including hex dumps,

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

strings, functions, permissions, control flow graphs, API calls, and metadata (Alghamdi, Alkinoon, Alghuried, & Mohaisen, 2024).

F. Smart Grid (SG)

A smart grid (SG) is a framework that controls the computer, and automation to address existing challenges in smart grid communication 5G enhances Smart Grids (SGs) by enabling real-time communication, improving automation, scalability, and efficiency. Secure authentication, including 5G-AKA, protects against unauthorized access and cyber threats (Sali, Al-Jumaily, Jiménez, & Al-Jumeily, 2023). To strengthen SG communication, a password-based anonymous lightweight key agreement framework has been proposed, addressing security challenges in smart grid systems. The security of the PALK has been proved by the random oracle model. PALK has the necessary security and functionalities under the CK adversary model. PALK has strong anonymity, data confidentiality, non-traceability, perfect forward secrecy mutual authentication, etc. in informal security analysis. Further, we have used the simulation tool "AVISPA" to show the PALK security against man-in-the-middle and replay attacks (Khan, Kumar, Ahmad, Rana, & Mishra, 2020).

The ISG-SLAS, a secure and lightweight authentication scheme for industrial SG using a fuzzy extractor. Key features include resistance to major attacks and robust security functionalities. Validation through ROR model, AVISPA simulation, and real-world tests using Raspberry Pi4 (Dargaoui et al., 2025).

Two-layer security paradigm for smart grid communication is proposed in this work. While the second layer uses node-to-node authentication using a one-class SVM method to identify anomalies, the first layer uses asymmetric encryption and randomized packet transmission to guarantee safe data exchange. To improve scalability, encryption, and packet sequencing are handled by two partly trusted servers (TTP). Real-time insights are obtained through the integration of SCADA and AMI systems; yet this paradigm successfully reduces the cyber security threats that are introduced. With little complexity, the method guarantees improved data security, scalability, and system stability (Parvez et al., 2024).

Smart Grids integrate IoT and Wireless Sensor Networks (WSNs) to improve energy efficiency and automation but face substantial cyber security threats. This analysis explores cyber security in Smart Grids, focusing on safeguarding WSNs from cyber-attacks that could disrupt stability and security. The underscores methods for attack prevention, secure communication, and maintaining privacy, integrity, and accessibility to create a dependable and secure Smart Grid framework (Aghmadi, Hussein, Polara, & Mohammed, 2023).

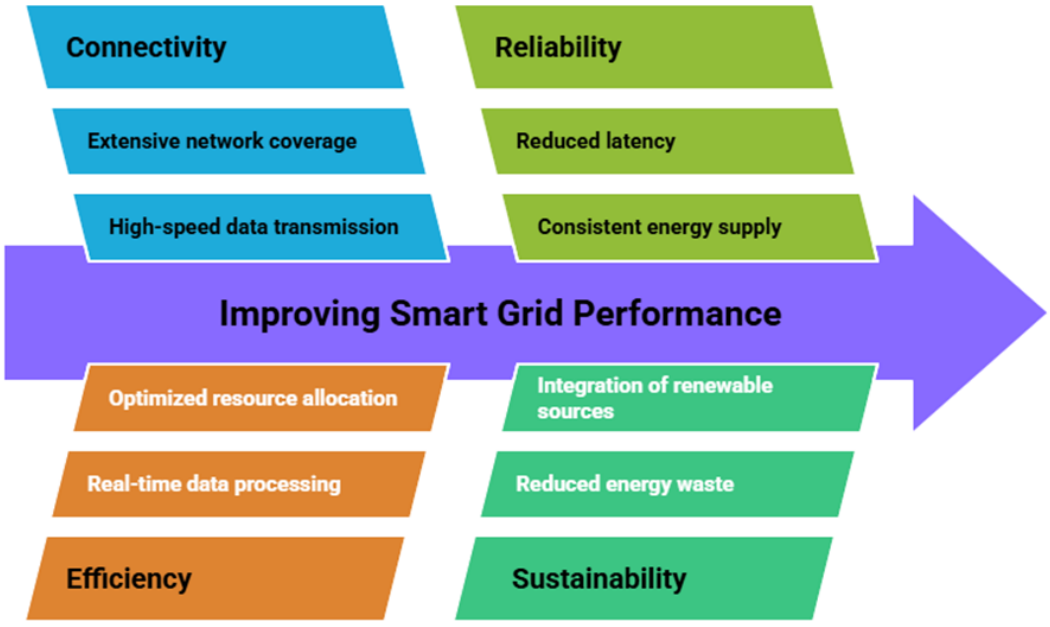

Figure 7: Unveiling 5G impact on smart grids.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

G. Vehicle ad hoc network (VANET)

5G enhances VANETs with real-time traffic management and collision avoidance, requiring strong authentication like 5G-AKA to prevent cyber threats. Challenges include high mobility, scalability, and lightweight security. The rise in EVs adds risks to pay-and-charge systems, as Charging Stations handle sensitive data with existing solutions not fully addressing threats like impersonation and privacy breaches. An advancement of VANET, the Internet of Vehicles (IoV), improves communication among vehicles, RSUs, and automobiles in smart cities conventional VANETs use DSRC, which has drawbacks such as high latency and poor scalability. LTE-V offers better capacity, mobility, and spectral efficiency for V2X communication with low scalability, presented a lightweight group key agreement and certificate-less authentication solution for LTE-V that includes certificate-less authentication based on elliptic curves for data integrity and privacy. RSU computational burden can be decreased with batch verification. Distributing group keys dynamically allows for effective updates with less processing power. The scheme is semantically secure under the Random Oracle Model (ROM) and resists adversarial attacks (Lv, Qin, Gan, Xu, & Shi, 2024).

Through vehicle connectivity and data sharing, the Internet of Vehicles (IoV) improves road safety, eases congestion, and improves traffic management. Protecting privacy, providing quick Vehicle-to-Everything (V2X) connectivity, and handling large data are some of the main obstacles. IoV performance optimization, traffic forecasting, and congestion reduction are some of the answers provided by machine learning (ML). Reviewing machine learning (ML) and deep reinforcement learning (DRL) for the Internet of Vehicles (IoV), this research focuses on employing Markov Decision Processes (MDP) for energy-aware optimization and safe edge computing offloading for job management. IoV systems utilizing ML and V2X technologies that are scalable, secure, and energy-efficient are examples of future directions (Taslimasa et al., 2023).

The VANETs, a cluster-based routing protocol to improve routing performance and thwart black hole assaults. An ANN model detects malicious nodes with 98.97% accuracy. Secure clusters are created, and route discovery is optimized using a modified AODV protocol, increasing network speed and decreasing latency. Although successful, the study focuses on specialized convoy operations and black hole assaults. Nature enhancements will leverage reinforcement learning to enable secure and low-latency vehicle-to-vehicle (V2V) communication (Suganya & Prakash, 2024).

A bilinear pairing-based anonymous authentication scheme that enhances security and efficiency in 5G-assisted vehicular fog computing. It ensures conditional privacy, reduces computational overhead by omitting map-to-point functions, and optimizes bilinear pairing operations. The scheme is resilient against impersonation, replay, and man-in-the-middle attacks, verified through security analyses and tools like AVISPA. Future work includes quantum-resistant cryptography, machine learning-based anomaly detection, and scalability testing for large vehicular networks in 6G environments (Almazroi et al., 2024).

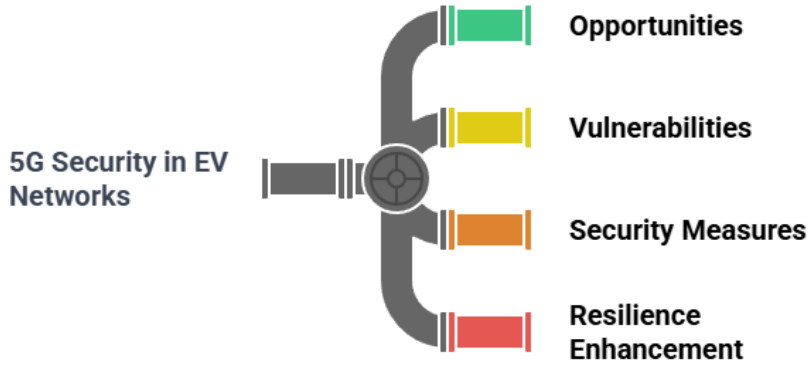

Figure 8: Navigating 5G security in EV networks.

H. Wireless Sensor Networks (WSNs)

5G is larger-threats including illicit access and data breaches because the amount of connected 5G is largely dependent on Wireless Sensor Networks (WSNs) to provide smart applications like healthcare and smart cities.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Nevertheless, there are security concerns with their integration into 5G, especially in relation to authentication. WSN nodes' limited resources may make traditional authentication techniques insufficient. Advanced methods including blockchain, lightweight cryptographic protocols, and AI-driven anomaly detection are being investigated to improve security. Increasing authentication guarantees secure connection, safeguarding confidentiality and data integrity in 5G-powered WSNs. This research proposes a unique four-factor authentication technique to improve communication security in Wireless Sensor Networks (WSNs) inside the Internet of Things (IoT) ecosystem, used fingerprints, random numbers (nonce), timestamps, and holomorphic encryption to provide strong user authentication. It may be used in a variety of settings, including banking, healthcare, education, and online shopping, To combat identity theft and ensure safe data transfer over public networks (Alghamedy et al., 2024).

Securing multi-group communication is necessary for wireless sensor networks, but current key management systems have a complex lack of efficiency the major issue in the context of overall communication cost during the membership update process in the multi-group scenario and storage computation overhead at the user's end during the re-keying process, suggested BP-MGKM for secure multi-group key management based on bi-variant polynomial. The method outperforms existing alternatives in terms of efficiency, re-keying complexity reduction, and security with resilience against different assaults like secrecy, resilience against node compromise attacks, collusion attacks, and replay attacks (Lalouani, Younis, & Tan, 2023).

The research highlights security flaws in Gupta et al.'s authentication strategy for TMIS and wearable sensor networks. The research suggests SHAPARAK, an authentication system that is both scalable and resistant to attacks, as a solution to these problems. It operates in a lightweight manner, guarantees anonymity and untraceability, and allows for password and biometric changes without the need for a reliable server. SHAPARAK provides improved security and efficiency, Future research will examine multi-server TMIS handovers and user ID updates in unsecured channels (Hosseinzadeh et al., 2024).

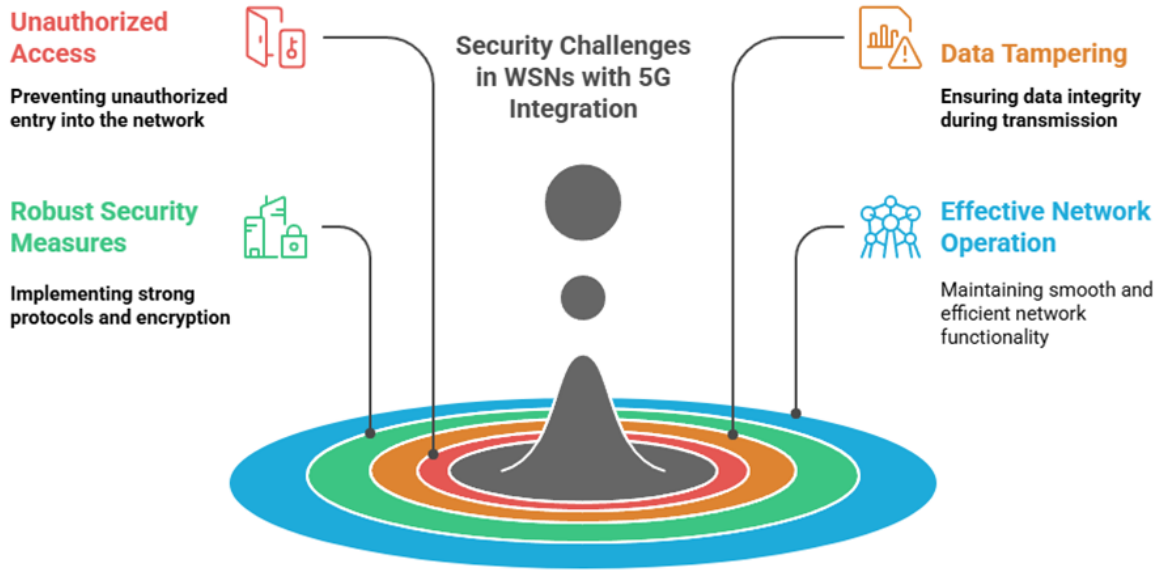

Figure 9: Security in Enhance WSNs.

Table 1: Overview of Security Enhancements and Protocols for 5G/6G Networks

Ref. No.	Application	Method	Contribution	Limitation	Attack Type
(Deebak & Al-Turjman, 2023)	Secure packet transmission in 5G/B5G/6G networks	Group Key utilizing Initial Key Agreement (GKIKA)	Ensures secure packet encryption/decryption using symmetric/asymmetric encryption, timestamps, and MACs. Protects against replay and manipulation.	Computational overhead in symmetric/asymmetric encryption.	Replay and manipulation

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Ref. No.	Application	Method	Contribution	Limitation	Attack Type
(Yadav et al., 2022)	Secure transmission in 5G	Cryptography, deep learning-based key generation	Balances security and transmission delay and protects against data leakage and replay risks using dynamic/static keys.	Dependency on UPF-specific optimizations for scalability.	Replay and tampering risks
(Hsiao et al., 2024)	Securing 5G networks	Protocol addressing impersonation, replay, and jamming threats	Provides safe handovers and mutual authentication while maximizing speed and reducing costs. Validated using AVISPA tools.	Limited exploration of specific jamming scenarios.	Impersonation, replay, and jamming
(You et al., 2023)	Integrating non-3GPP networks into 5G Core	EAP-based authentication	Safely incorporates WiFi into 5G, evaluates Eduroam roaming, and explores simultaneous authentication.	Requires further research on cross-network integration.	Authentication vulnerabilities
(Suresh Kumar et al., 2024)	User privacy in Mobile Virtual Network Operators (MVNOs)	Privacy-focused authentication and handover	Simplifies validation between MVNOs and MNOs while ensuring anonymity and unlinkability.	Limited analysis of cross-layer authentication mechanisms.	Privacy risks in MVNO handovers
(De Simone et al., 2024)	Improving 6G security	Decentralized Multi-Round Negotiation Protocol (DMRN)	Combines PQC and PFS while maintaining compatibility with 3GPP standards. Highlights weaknesses in the replay and HN masquerade attacks.	Replay and masquerade attacks require further improvements.	Replay and HN masquerade attacks
(Haghrah, Haghrah, Niya, & Ghaemi, 2023)	Secure 5G handovers	Secure handover protocol using fuzzy logic and spiking neural networks	Enhances forward secrecy, reduces handover time, and protects against various attacks.	Requires extensive computational resources for neural network-based decisions.	Handover-related attacks
(Kaada et al., 2024)	Enhancing 5G infrastructure resilience	Stochastic framework for availability and performance optimization	Focuses on high availability, minimal redundancy, and optimized resilience through stochastic reward networks.	Limited focus on real-world applicability in non-product-form queuing networks.	Node failure and delay-related vulnerabilities
(Rupanetti & Kaabouch, 2024)	IoT authentication for smart grids	Mutual authentication with PUFs	Ensures secure communication between smart meters and networks; more resilient to attacks; improves computational and communication efficiency.	Focused on smart grids; applicability to other domains is not discussed.	Physical, and cyber-attacks
(Tamilselvan, 2024)	Blockchain-based IoT authentication	Blockchain-assisted SKGPs	Highlights gaps in current research on SKGPs, evaluates protocols based on execution time, overhead, and security; and identifies potential cryptographic libraries for implementation.	Limited focus on real-world testing and implementation.	Replay, impersonation, node capture
(Thapliyal et al., 2024)	An IoT-enabled smart home systems	SA IoT-SL authenticated key agreement	Addresses energy waste and improves security; guarantees reliable connection between cloud servers, users, and sensors; validated with Scyther tool; effective in real-world applications.	Future improvements require integrating AI-based data analysis for forecasting.	Replay, impersonation, energy-related vulnerabilities

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Ref. No.	Application	Method	Contribution	Limitation	Attack Type
(Jin et al., 2024)	IoT Authentication	Cryptographic techniques (hash functions, elliptic curve)	Analyzed IoT authentication protocols (2019-2023) across domains (smart cities, healthcare, industry), offering improvements over current methods	Node capture, DoS attacks	Node capture, Denial of Service (DoS)
(Rupanetti & Kaabouch, 2024)	Edge Computing in IoT (EC-IoT)	AI-based approaches SA IoT-SL (Secure A IoT-enabled authenticated key agreement)	Developed a secure authentication system to reduce energy waste and enhance security in smart home settings, outperforming existing methods	Limited to smart home environments, integration with other systems	Man-in-the-middle, unauthorized access
(Nyangaresi, 2023)	Lightweight authentication for UAV sensors	Hash functions and quadratic residues	Addresses side routing, de-synchronization, and session leakage attacks; validated under ROM, Dolev-Yao, and CK threat models.	Limited compatibility with certain UAV sensors.	Side routing, de-synchronization, session leakage
(Li et al., 2024)	Secure authentication in satellite-UAV networks	Chebyshev polynomial and ECC-based public key cryptography	Resolves security issues in Space-Air-Ground 6G framework; counters eavesdropping, manipulation, and impersonation.	Challenges with propagation delays in satellite networks.	Eavesdropping, manipulation, impersonation
(Pu & Li, 2020)	Lightweight IoD authentication	PUFs, chaotic maps, and hash functions	Protects against impersonation and cloning; robust against IoD-specific attacks; enhances system performance.	Focused primarily on IoD-specific security risks; broader.	Impersonation, cloning

CHALLENGES

Quantum-resistant encryption, blockchain, artificial intelligence, and zero-trust security models will be the main drivers of cybersecurity in 5G. These technologies will be crucial for stopping cyberattacks, safeguarding user privacy, and making sure that communication networks are secure as 5G use grows.

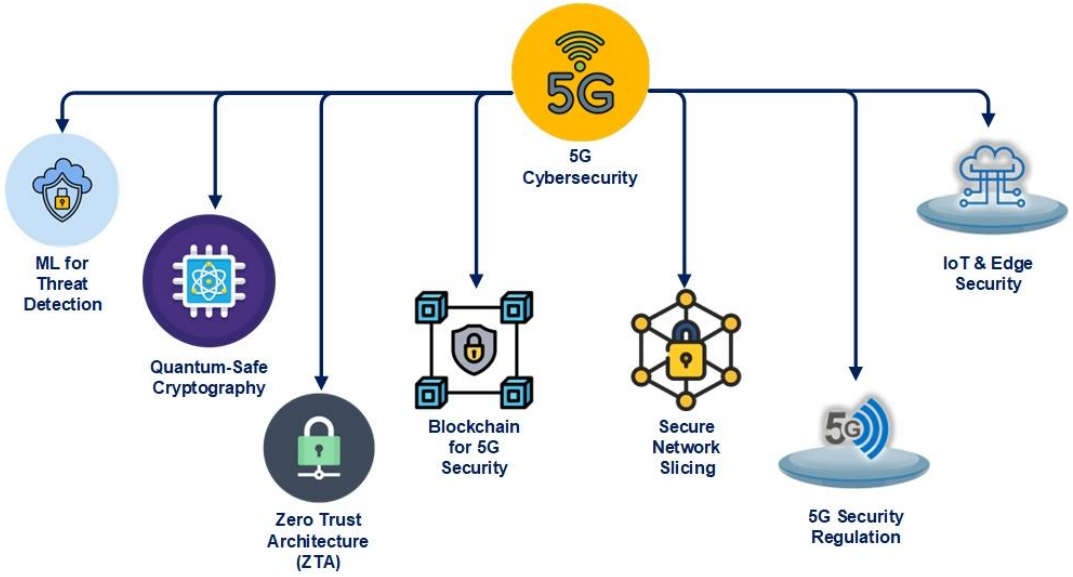

Figure 10: 5G cybersecurity prospects technology.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Technological Future Prospects for Cybersecurity Systems in 5G not only increase speed by increasing the number of connected devices attack surfaces, and connectivity but also pose cybersecurity challenges. AI and machine learning will be incorporated into future strategies for real-time threat identification and autonomous security (Fakhouri et al., 2023). The key elements of zero-trust security will be strict authentication and micro-segmentation. Advanced encryption, quantum-safe cryptography, blockchain authentication, and AI-powered anomaly detection will secure IoT, edge computing, and 5G network slicing. Blockchain will also ensure tamper-proof transactions and decentralized identity management and decentralized identity management (Geetanshi, Manocha, Babbar, & Mangla, 2025).

CYBERSECURITY SYSTEM

A cybersecurity system is a set of tools, processes, and practices used to safeguard digital networks, devices, apps, and data versus online attacks. It protects abilities alongside illegitimate access, data violations, and cyber-attacks and includes protections such as firewalls, encryption, and authentication (Aslan, Aktuğ, Ozkan-Okay, Yilmaz, & Akin, 2023). Also, with a wide structure of tools. Important destinations are to avoid illegal access, reduce data violations, and protect them from harmful cyber attacks, including the risk of phishing attacks, denial-of-service (DOS) attacks and fraudulent software. To gather strong security, the cybersecurity system integrates multiple defense layers, including:

- **Firewall:** Relieved obstacles between reliable internal networks and incredible external sources, filters incoming and outgoing traffic based on safety rules.
- **Encryption:** It protects sensitive data by converting them to unlimited codes and ensuring that even if the cutter gets them, the information remains unavailable without the decryption keys.
- **Authentication Mechanisms:** Check the user's identity through methods such as passwords, biometrics, multifactor authentication (MFA), and digital certificates to prevent certification mechanisms-monetary access.
- **Intrusion Detection and Prevention Systems (IDPS):** Monitor network traffic for suspicious activity and automatically block potential threats.
- **Endpoint Protection:** Antivirus software, patch administration, and behavioral analysis protect individual devices (computers, smartphones, and IoT devices).
- **Security Policy and Training in Employees:** Establish guidelines for secure digital practice and educate users to recognize and avoid cyber threats.

In addition, the cybersecurity system depends on continuous monitoring, danger information, and response plans for the incident to develop risk and reduce injuries in case of violation. As cyber threats are more sophisticated, organizations should use adaptive, active security measures to ensure flexibility against attacks.

NOVELTY

This article presented an extensive evaluation of the emerging risks and authentication mechanisms in 5G networks, providing an integrated perspective on the cutting edge of 5G security. This investigation is exceptional due to it does an exhaustive investigation of the evolving threat spectacle and delves further into advanced authentication systems focused on addressing these demanding concerns. Furthermore, this research includes a comprehensive and forward-looking review of 5G authentication approaches and possible future risks (Agrawal, Agrawal, Bomanwar, Dubey, & Jaiswal, 2023). Integrating recent research and advanced technologies provides a valuable resource for academics, policymakers, and practitioners aiming to secure 5G networks. This contemporary significant addition to the field of 5G cybersecurity is driven by an emphasis on lightweight solutions, privacy enhancements, real-time attack mitigation, and chaotic structures.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

1. Chaotic Systems

The integration of chaotic patterns into authentication processes is investigated as a novel approach to improving security in 5G networks. Chaotic systems, due to their characteristic predictability and sensitivity to the initial circumstances, provide advantages for dynamic key technology and secure discussion, especially in restricted resource scenarios (Fazrina, 2024).

2. Threat Setting Analysis

A unique and up-to-date evaluation of the emerging risks in 5G networks is provided, inclusive of impersonation attacks, signaling storms, and man-in-the-middle (MitM) attacks. This evaluation synthesizes contemporary research to provide a comprehensive view of the vulnerabilities and attack vectors irregular to 5G, presenting precious insights for researchers and practitioners.

3. Integration of Advanced Authentication Mechanisms

Advanced authentication protocols, consisting of the 5G Authentication and Key Agreement (5G-AKA) protocol, are reviewed, and compared, with improvements such as Elliptic Curve Cryptography (ECC), quantum-resistant encryption, and blockchain-primarily based authentication investigated. The capability of those advanced techniques to manage with the rules of traditional authentication mechanisms in 5G networks is highlighted.

4. IoT and Resource-Constrained Devices

A fundamental novelty is the emphasis on lightweight and scalable authentication systems designed specifically for Internet of Things (IoT) devices and other resource-constrained situations. Protocols that promote stability and efficiency are discussed, offering strong protection for low-power devices while minimizing computational and communication overhead.

5. Emerging Technologies

Emerging technologies such as AI-based complete anomaly detection, blockchain, and quantum-resistant cryptography are investigated, going beyond traditional authentication approaches. A forward-thinking view is provided on how these technologies might be incorporated into 5G networks to improve safety and handle future threats.

6. Cross-Domain Applications

Authentication procedures across a wide range of 5G-enabled tasks, including smart cities, autonomous vehicles, healthcare, and commercial automation, are investigated. Examining the specific safety requirements of various domains, domain-specific insights are offered that are not typically covered in normal evaluations of 5G security.

7. Comparison of Authentication Protocols

A significant addition is the comparative examination of several authentication systems, which highlights their strengths, shortcomings, and applicability for specific 5G use cases. This review provides a significant and useful resource for stakeholders looking to select or layout authentication solutions for specific applications.

8. Privacy and Anonymity

Privacy-sensitive scenarios in 5G networks, notably in terms of person and tool anonymity, are addressed. Innovative techniques such as Variable Radio Network Temporary Identifier (V-RNTI) and pseudonym-based authentication are examined, to improve privacy while maintaining security.

9. Real-Time Threat Mitigation

Real-time risk detection and mitigation strategies are investigated, highlighting the importance of adaptive authentication and the dynamic key era in responding to developing threats. This focus on real-time security distinguishes this assessment from others.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

10. Compatible with Existing Standards

The importance of maintaining compatibility with current 3GPP criteria is brought up, as are improvements to 5G systems for authentication. This ensures that the investigated solutions will be readily integrated into future 5G networks without requiring significant modifications.

Table 2. Main abbreviations

Abbreviation	Meaning
5GAKA	5G Authentication and Key Agreement
5GC	5G Core
AES	Advanced Encryption Standard
AMF	Mobility management
CSP	Cloud Service Provider
DDHP	Decisional Diffie-Hellman problem
DRL	Deep reinforcement learning
EC	Edge Computer
ECDH	Elliptic Curve Diffie-Hellman
FANETs	Flying Ad-hoc Networks
FCCM	Fractional Chebyshev Chaotic Map
GKIKA	Group Key utilizing Initial Key Agreement
IoD	Internet of Drones
KCIA	Key Compromise Impersonation
KFS/KBS	Key Forward/Backward Secrecy
LAPEC	Lightweight Authentication Protocol
LS-AKA	Location Services Authentication and Key Agreement
MDP	Markov Decision Processes
MitM	Man-in-the-middle
NSSF	Network Slicing
OFMC	Open-Source Finite Model Checking
PDCA	Plan-Do-Check-Action
PPRU	Privacy-Preserving Reputation Updating
PUFs	Physical Unclonable Functions
RFID	Radio Frequency Identification
ROR	Real-Or-Random
SBGR	Secure Bit Generation Rates
SN	Serving Network
SSTI	Session State Temporal Insensitivity
TCN	Temporal Convolutional Networks
UE	User Equipment
V-RNTI	Variable Radio Network Temporary Identifier
WSNs	Wireless Sensor Networks

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

CONCLUSION

Authentication is a key element of 5G application security, ensuring that only authorized users and devices may connect to the network. Numerous applications, such as augmented reality, smart cities, autonomous cars, the Internet of Things, and healthcare, require robust security measures. The 5G security system is considerably strengthened by elite technologies including dynamic identity verification, high-level encryption techniques, and mutual authentication protocols. However, there are a number of difficulties due to the expanded attack surface and related risks, including device impersonation, replay assaults, and data breaches. Advanced authentication techniques these solutions improve user privacy, strengthen identity verification and prevent unwanted access. To satisfy the computational and energy efficiency requirements of 5G devices, Frameworks for scalable and lightweight authentication are very crucial. Moreover, the highly connected and complex character of the 5G application demands continuous updates of authentication security for addressing emerging risks and adaptive attacks. By prioritizing authentication security, stakeholders can ensure the seamless operation of 5G technologies while maintaining trust and confidence across industries and users. Finally, creating a safe ecosystem for 5G applications not only improves user experience but also paves the way for the long-term growth and success of this revolutionary technology.

Acknowledgment:

The authors declare no conflicts of interest in this research. Furthermore, the funders were not involved in the study's design, data collection, analysis, interpretation, manuscript writing, or decision to publish.

Author Contributions:

Conceptualization, IJMK; methodology, validation, formal analysis, IJMK and JM; investigation, resources, data curation, and IJMK; KJM and MHA; writing original draft preparation, IJMK and AAJ; writing review and editing, IJMK and AAJ; visualization, JM; supervision, JM; project administration, JM; funding acquisition. All authors have read and agreed to the published version of the manuscript.

Conflicts of Interest:

There are no conflicts of interest disclosed by the authors. There were no non-financial or financial relationships that affected the research and this study did not receive any outside funding.

REFERENCES

[1] Abid, N. A Review of Security and Privacy Challenges in Augmented Reality and Virtual Reality Systems with Current Solutions and Future Directions. *Emerging Technologies in AI and Machine Learning*.

[2] Aghmadi, A., Hussein, H., Polara, K. H., & Mohammed, O. (2023). A comprehensive review of architecture, communication, and cybersecurity in networked microgrid systems. *Inventions, 8*(4), 84.

[3] Agrawal, V., Agrawal, S., Bomanwar, A., Dubey, T., & Jaiswal, A. (2023). Exploring the risks, benefits, advances, and challenges in internet integration in medicine with the advent of 5G technology: A comprehensive review. *Cureus, 15*(11).

[4] Al-Jumaily, A., Alrubaee, S. H., Jiménez, V. P. G., Al-Saegh, A. M., Mahmood, A. A., & Al-Jumeily, D. (2023). *Architecture design of B5G and 6G millimeter-wave radio access network: Using wireless communications to increase coverage, capacity and performance*. Paper presented at the 2023 16th International Conference on Developments in eSystems Engineering (DeSE).

[5] Al-Jumaily, A., Sali, A., Riyadh, M., Wali, S. Q., Li, L., & Osman, A. F. (2023). Machine learning modeling for radiofrequency electromagnetic fields (RF-EMF) signals from mmwave 5G signals. *IEEe Access, 11*, 79648-79658.

[6] Alghamdi, A., Alkinoon, A., Alghuried, A., & Mohaisen, D. (2024). xr-droid: A Benchmark Dataset for AR/VR and Security Applications. *IEEE Transactions on Dependable and Secure Computing*.

[7] Alghamedy, F. H., El-Haggar, N., Alsumayt, A., Alfawaer, Z., Alshammari, M., Amouri, L., . . . Albassam, S. (2024). Unlocking a Promising Future: integrating Blockchain Technology and FL-IoT in the journey to 6G. *IEEe Access*.

[8] Almazroi, A. A., Alqarni, M. A., Al-Shareeda, M. A., Alkinani, M. H., Almazroey, A. A., & Gaber, T. (2024). A Bilinear Pairing-Based Anonymous Authentication Scheme for 5G-Assisted Vehicular Fog Computing. *Arabian Journal for Science and Engineering*, 1-22.

[9] Alnashwan, R., Yang, Y., Dong, Y., Gope, P., Abdolmaleki, B., & Hussain, S. R. (2024). *Strong privacy-preserving universally composable aka protocol with seamless handover support for mobile virtual network operator*. Paper presented at the Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security.
[10] Ananthula, B., & Budde, N. (2023). The deeper investigation of smarthealthcare systems using 5G Security. In.
[11] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics, 12*(6), 1333.
[12] Benfarhi, Z. (2024). Evaluation of a New Authentication and Key Agreement Protocol for 5G Network. In: Final International University.
[13] Cekerevac, Z., Cekerevac, P., Prigoda, L., & Al-Naima, F. (2025). SECURITY RISKS FROM THE MODERN MAN-IN-THE-MIDDLE ATTACKS. *MEST Journal, 13*(1).
[14] Chander, B., & Gopalakrishnan, K. (2022a). RFID tag-based mutual authentication protocol with improved security for TMIS. *International Journal of Information and Computer Security, 18*(3-4), 383-405.
[15] Chander, B., & Gopalakrishnan, K. (2022b). A secured and lightweight RFID-tag based authentication protocol with privacy-preserving in Telecare medicine information system. *Computer Communications, 191*, 425-437.
[16] Damir, M. T., Meskanen, T., Ramezanian, S., & Niemi, V. (2022). *A beyond-5G authentication and key agreement protocol*. Paper presented at the International Conference on Network and System Security.
[17] Dargaoui, S., Azrour, M., El Allaoui, A., Guezzaz, A., Alabdulatif, A., & Ahmad, S. (2025). ECC-Based Anonymous and Multi-factor Authentication Scheme for IoT Environment. *International Journal of Online & Biomedical Engineering, 21*(1).
[18] De Simone, L., Di Mauro, M., Natella, R., & Postiglione, F. (2024). Performance and availability challenges in designing resilient 5g architectures. *IEEE Transactions on Network and Service Management*.
[19] Deebak, B., & Al-Turjman, F. (2023). Secure-user sign-in authentication for IoT-based eHealth systems. *Complex & Intelligent Systems, 9*(3), 2629-2649.
[20] Fakhouri, H. N., Alawadi, S., Awaysheh, F. M., Hani, I. B., Alkhalaileh, M., & Hamad, F. (2023). A comprehensive study on the role of machine learning in 5G security: Challenges, technologies, and solutions. *Electronics, 12*(22), 4604.
[21] Fazrina, N. (2024). Securing Distributed Sensor Systems Through Adaptive Encryption Algorithms in 5G-Based Smart Energy Networks. *Open Journal of Robotics, Autonomous Decision-Making, and Human-Machine Interaction, 9*(11), 18-27.
[22] Geetanshi, Manocha, H., Babbar, H., & Mangla, C. (2025). Securing the Internet of Things: Cybersecurity Challenges, Strategies, and Future Directions in the Era of 5G and Edge Computing. *Current and Future Cellular Systems: Technologies, Applications, and Challenges*, 89-106.
[23] Gil Jiménez, V., Al-Jumaily, A., Sali, A., & Al-Jumeily, D. (2023). Hybrid Chaos Particle Swarm Optimization algorithm for smart Cloud Service System based on optimization resource scheduling and allocation. *Journal of Autonomous Intelligence, 6*(2), 652-652.
[24] Gupta, S., Pradhan, A. K., Chaudhari, N. S., & Singh, A. (2023). LS-AKA: a lightweight and secure authentication and key agreement scheme for enhanced machine type communication devices in 5G smart environment. *Sustainable Energy Technologies and Assessments, 60*, 103448.
[25] Hafeez, M. A., Shakib, K. H., & Munir, A. (2025). A Secure and Scalable Authentication and Communication Protocol for Smart Grids. *Journal of Cybersecurity and Privacy, 5*(2), 11.
[26] Haghrah, A., Haghrah, A., Niya, J. M., & Ghaemi, S. (2023). Handover triggering estimation based on fuzzy logic for LTE-A/5 G networks with ultra-dense small cells. *Soft Computing, 27*(22), 17333-17345.
[27] Hatami, M., Qu, Q., Chen, Y., Kholidy, H., Blasch, E., & Ardiles-Cruz, E. (2024). A Survey of the Real-Time Metaverse: Challenges and Opportunities. *Future Internet, 16*(10), 379.
[28] Hojjati, M., Shafieinejad, A., & Yanikomeroglu, H. (2020). A blockchain-based authentication and key agreement (AKA) protocol for 5G networks. *IEEe Access, 8*, 216461-216476.
[29] Hosseinzadeh, M., Servati, M. R., Rahmani, A. M., Safkhani, M., Lansky, J., Janoscova, R., . . . Lee, S.-W. (2024). An enhanced authentication protocol suitable for constrained RFID systems. *IEEe Access, 12*, 61610-61628.
[30] Hsiao, L.-S., Tsai, K.-L., Liu, J.-C., Leu, F.-Y., Lu, Y.-S., & Lin, I.-L. (2024). Security among UPFs belonging to Different 5G/B5G/6G Networks. *Information Systems Frontiers*, 1-12.

[31] Jin, X., Lin, N., Li, Z., Jiang, W., Jia, Y., & Li, Q. (2024). A Lightweight Authentication Scheme for Power IoT Based on PUF and Chebyshev Chaotic Map. *IEEe Access*.
[32] Kaada, S., Tran, D.-H., Van Huynh, N., Morel, M.-L. A., Jelassi, S., & Rubino, G. (2024). Multi-Agent Deep Reinforcement Learning for Resilience Optimization in 5G RAN. *arXiv preprint arXiv:2407.18066*.
[33] Khalaf, A. G., & Mohammed, K. J. (2024). *Using thermal bands of landsat images to analysis the land surface temperature in Dewaniya region of Iraq*. Paper presented at the AIP Conference Proceedings.
[34] Khan, A. A., Kumar, V., Ahmad, M., Rana, S., & Mishra, D. (2020). PALK: Password-based anonymous lightweight key agreement framework for smart grid. *International Journal of Electrical Power & Energy Systems, 121*, 106121.
[35] Kumar, A. S., Kumar, A. R., Manoranjithem, V., & Gottumukkala, P. (2024). *A Secure and Efficient Key Management for Intrusion Detection In Cloud Storage Based On PLS And SVM Model.* Paper presented at the 2024 International Conference on Integration of Emerging Technologies for the Digital World (ICIETDW).
[36] Kwon, D., & Park, Y. (2024). Design of Secure and Efficient Authentication Protocol for Edge Computing-Based Augmented Reality Environments. *Electronics, 13*(3), 551.
[37] Lalouani, W., Younis, M., & Tan, D. (2023). *Lightweight and Anonymity-preserving Secure Group Communication Mechanism for Cooperative Driving*. Paper presented at the 2023 32nd Wireless and Optical Communications Conference (WOCC).
[38] Li, S., Cao, J., Shi, X., & Li, H. (2024). Enabling Space-Air integration: A Satellite-UAV networking authentication scheme. *Security and Safety, 3*, 2023030.
[39] Lv, S., Qin, Y., Gan, W., Xu, Z., & Shi, L. (2024). A systematic literature review of vehicle-to-everything in communication, computation and service scenarios. *International Journal of General Systems, 53*(7-8), 1042-1072.
[40] Mahmood, K., Ayub, M. F., Hassan, S. Z., Ghaffar, Z., Lv, Z., & Chaudhry, S. A. (2022). A seamless anonymous authentication protocol for mobile edge computing infrastructure. *Computer Communications, 186*, 12-21.
[41] Mookherji, S., Odelu, V., & Prasath, R. (2024). Secure ultra fast authentication protocol for electric vehicle charging. *Computers and Electrical Engineering, 119*, 109512.
[42] Mutlaq, K. A.-A., Nyangaresi, V. O., Omar, M. A., Abduljabbar, Z. A., Abduljaleel, I. Q., Ma, J., & Al Sibahee, M. A. (2024). Low complexity smart grid security protocol based on elliptic curve cryptography, biometrics and hamming distance. *PloS one, 19*(1), e0296781.
[43] Nyangaresi, V. O. (2023). Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. *High-Confidence Computing, 3*(4), 100154.
[44] Nyangaresi, V. O., Alsolami, E., & Ahmad, M. (2024). Trust-enabled Energy Efficient Protocol for Secure Remote Sensing in Supply Chain Management. *IEEe Access*.
[45] Parvez, I., Aghili, M., Riggs, H., Sundararajan, A., Sarwat, A. I., & Srivastava, A. K. (2024). A Novel Authentication Management for the Data Security of Smart Grid. *IEEE Open Access Journal of Power and Energy*.
[46] Pu, C., Choo, K.-K. R., & Korać, D. (2024). A lightweight and anonymous application-aware authentication and key agreement protocol for the internet of drones. *IEEE Internet of Things Journal*.
[47] Pu, C., & Li, Y. (2020). *Lightweight authentication protocol for unmanned aerial vehicles using physical unclonable function and chaotic system*. Paper presented at the 2020 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN.
[48] Rupanetti, D., & Kaabouch, N. (2024). Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities. *Applied Sciences, 14*(16), 7104.
[49] Saeed, M. M., Hasan, M. K., Obaid, A. J., Saeed, R. A., Mokhtar, R. A., Ali, E. S., . . . Hossain, A. Z. (2022). A comprehensive review on the users' identity privacy for 5G networks. *IET Communications, 16*(5), 384-399.
[50] Sali, A., Al-Jumaily, A., Jiménez, V. P. G., & Al-Jumeily, D. (2023). Cybersecurity threat perception technology based on knowledge graph. *Journal of Autonomous Intelligence, 6*(3).
[51] Shah, S. F. A., Mazhar, T., Al Shloul, T., Shahzad, T., Hu, Y.-C., Mallek, F., & Hamam, H. (2024). Applications, challenges, and solutions of unmanned aerial vehicles in smart city using blockchain. *PeerJ Computer Science, 10*, e1776.
[52] Suganya, R., & Prakash, B. (2024). *Optimizing Vanet Communications: A Bibliometric Analysis of Energy-Efficient Strategies with Deep Learning*. Paper presented at the 2024 International Conference on System, Computation, Automation and Networking (ICSCAN).

Research Article

[53] Suresh Kumar, V., Ibrahim Khalaf, O., Raman Chandan, R., Bsoul, Q., Kant Gupta, S., Zawaideh, F., . . . Salama AbdElminaam, D. (2024). Implementation of a novel secured authentication protocol for cyber security applications. *Scientific Reports, 14*(1), 25708.

[54] Susanto, H., & Leu, F.-Y. (2022). *Asymmetric Cryptography Among Different 5G*. Paper presented at the Innovative Mobile and Internet Services in Ubiquitous Computing: Proceedings of the 16th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS-2022).

[55] Tamilselvan, N. (2024). Blockchain-based digital rights management for enhanced content security in digital libraries. *International Journal of Blockchain Technology (IJBT), 2*(1), 1-8.

[56] Taslimasa, H., Dadkhah, S., Neto, E. C. P., Xiong, P., Ray, S., & Ghorbani, A. A. (2023). Security issues in Internet of Vehicles (IoV): A comprehensive survey. *Internet of Things, 22*, 100809.

[57] Thapliyal, S., Wazid, M., Singh, D. P., Chauhan, R., Mishra, A. K., & Das, A. K. (2024). Secure Artificial Intelligence of Things (AIoT)-enabled authenticated key agreement technique for smart living environment. *Computers and Electrical Engineering, 118*, 109353.

[58] Xiao, W., Liu, B., & Yin, W. (2024). Security authentication scheme based on chebyshev chaotic mapping for library network. *Alexandria Engineering Journal, 109*, 262-269.

[59] Xiao, Y., & Wu, Y. (2022). 5g-ipaka: An improved primary authentication and key agreement protocol for 5g networks. *Information, 13*(3), 125.

[60] Yadav, A. K., Misra, M., Pandey, P. K., Kaur, K., Garg, S., & Chen, X. (2022). *A provably secure ECC-based multi-factor 5G-AKA authentication protocol*. Paper presented at the GLOBECOM 2022-2022 IEEE Global Communications Conference.

[61] You, I., Kim, G., Shin, S., Kwon, H., Kim, J., & Baek, J. (2023). 5G-AKA-FS: A 5G authentication and key agreement protocol for forward secrecy. *Sensors, 24*(1), 159.

[62] You, I., Kim, J., Pawana, I. W. A. J., & Ko, Y. (2024). Mitigating Security Vulnerabilities in 6G Networks: A Comprehensive Analysis of the DMRN Protocol Using SVO Logic and ProVerif. *Applied Sciences, 14*(21), 9726.

[63] Yu, S., Lee, J., Sutrala, A. K., Das, A. K., & Park, Y. (2023). LAKA-UAV: Lightweight authentication and key agreement scheme for cloud-assisted Unmanned Aerial Vehicle using blockchain in flying ad-hoc networks. *Computer networks, 224*, 109612.

[64] Zhang, L., Wu, T., Liu, J., Guan, Z., & Yin, X. (2024). An Adaptive Synchronous Lightweight AKA Protocol With Authority Management for Wireless Medical Sensor Networks. *IEEE Systems Journal*.

[65] Zhang, S., Liu, Y., Han, Z., & Yang, Z. (2023). A lightweight authentication protocol for UAVs based on ECC scheme. *Drones, 7*(5), 315.