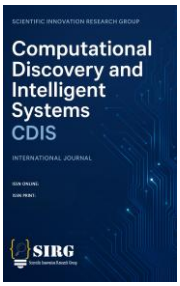
SIRG Scientific Innovation Research Group

Computational Discovery and Intelligent Systems (CDIS)

ISSN: XXXX-XXXX

Journal Homepage:
https://pub.scientificirg.com/index.php/CDIS/en/index



Cite this: CDIS, xxxx (xx), xxx

Comprehensive Analysis of Security Challenges and Mitigation Strategies in 5G Mobile Wireless Networks

***Ahmed Hammad*[*1], *Arwa Saad*[2], *Amer Ibrahim*[3] , *Ahmed A. Elnga*[4]**

*[*1] Faculty of Information Technology, Department of Computer Science, Al-Isra University, Amman, Jordan, (ahmed.khairt@iu.edu.jo)*

[2] Faculty of Computer Science, Nahda University, Beni Suef, Egypt, *(arwasaad812@gmail.com)*

[3]Department of Computer Science and Software Engineering, United Arab Emirates University, Al-Ain, UAE, (Amer.ibrahim@uaeu.ac.ae)

[5]Faculty of Computers and Artificial Intelligence, Beni-Suef University, Beni-Suef City, 62511, Egypt, (elngar_7@yahoo.co.uk)

**Corresponding Author: Ahmed Hammad[*1], (ahmed.khairt@iu.edu.jo)*

Abstract - The year 2025 will be a markedly more enriched and complex one in the communication network and service environment than the present scenario. The existing telecommunication technologies are expected to undergo upsurged enhancements, such as changed radio interaction and spectrum, with the emergence of 5th Generation (5G) mobile communication. The persistent and increasing need for multiple applications like massive access to the device, low latency, ultra-high bandwidth, reliability, etc., is met using enormous ground-breaking technologies embraced by the 5G network. Simultaneously, the core network and the logical layer on which the traditional security throws its light are no longer compatible with the 5G Mobile wireless network. Various factors like architectural errors, poor execution of communication protocol, exchange of metadata information, and so on, could be a menace to security and privacy if 5G Mobile wireless networks are programmed to execute all their activities in a secure platform. Furthermore, new privacy issues might arise due to its complexity and inadaptability due to the rapid change and the present communication infrastructure's tendency. 5G security also requires physical layer security as a part of it. However, the unavailability of proper research on vulnerabilities across all layers in 5G contributes primarily to security research findings at each layer. Correspondingly, potential security threats have failed to generate automated solutions. In the perception of an automated attack detection model, this article conducts a detailed research study of 5G security, incorporating the physical and logical layers to provide an automated solution for 5G security.

Received: 20 July 2025
Revised: 15 September 2025
Accepted: 30 October 2025
Available online: 22 December 2025

Keywords:

- 5G,
-Mobile Wireless Communication,
- Security,
- Data Privacy,
- Attacks.

Introduction

Today, the major contributors to the world's economy rely heavily on state-of-the-art Information Technology with its recent innovations in the communication sector [1]. In the

DOI: https://doi.org/XXXX.XXXX

merchandise and economy, information communication systems have secured a significant place. The limitations of conventional communication systems are overcome by the broad categories of supporting systems conceived in wireless mobile communications that consecutively empower global economic systems [2]. A massive transformation of the past generations in various scopes, such as reliability, efficacy, and acceleration, is expected with the advent of 5G and the New Radio (NR) technology [3]. The standards of 5G have been bringing reasonable improvement from past generations since its inception in 2020 [4]. This is to reinforce conventional cellular networks and a new sort of end nodes, like IoT and cooperative vehicles. New technologies will be introduced by NR that would, for example, support broader bandwidth and tremendous speeds. The global mobile devices increased from 10.5 billion in 2020 to 20 billion by 2025, maintaining wireless and mobile devices traffic of approximately 87.8 exabytes per month. The 5G network would adopt more ground-breaking technologies to reach its goal of "Internet of Everything" for enabling varied applications and services like e-Healthcare, AR, VR, IoT, Device-to-Device communications, Financial Technology, and Machine-to-Machine communications [5].

This paper throws light on 5G to depict its central idea, framework, and conventions with distinct layers and security confrontation, and its prospects. Security becomes the first-hand priority of stakeholders while developing 5G vertical applications because many security risks emerge from the latest 5G technology and performance-based unique application scenarios. In the following aspects, this paper makes its contributions [6]:

5G security falls short of an automated threat detection and response mechanism. Discovering a solution for automated attack-based 5G security is the main objective of this article. The 5G core network should be incorporated with the automated security mechanism [7].

The remaining paper is organized in the following manner: Section I briefly introduces 5G wireless mobile network security and the problem statement. Section II describes the review of the current literature on the subject. Section III briefs 5G Architecture and security model's provision of security mechanisms. The Automated Attack Detection Framework of 5G is described in Section IV. Section V contains the response to the research analysis of this paper, and finally, Section VI, the conclusion [8].

Literature review

Security architectures (e.g., 3GPPP TS 33.401) are often the label given to ready-made security solutions in the literature [9]. Instead of our security architecture, such architecture serves quite distinct purposes, viz., description of the security controls implementation and the ways to compile them. Nonetheless, there is a need for a toolbox and guidance that enables us to model the system itself as a whole with security at the center point for developing security solutions specifically for the designed system from scratch [10]. These things are to be considered while designing systems such as 5G with a wide range of distinct intentions. For the instantiation of secure systems, a methodology named security architecture is defined in this paper. This methodology contains a toolbox for apt modeling of security systems, security design principles, a set of security functions, and a mechanism for executing the security controls required to meet system security goals [11]. The security architecture in ITU-T X.805 supports this perception of security architecture. X. 805 specifically stated that "there is a logical division of a difficult set of features similar to back-to-back network security into independent architectural elements." Hence, "an organized method to back-to-back security is permitted by this independence, which can be adopted for framing a new security solution besides the current networks' security assessment."

The author [12] replaced the design for RANs to imitate the challenges and problems of backhaul. Moreover, the essentials of backhaul LTE were introduced by Raza and Networks, and they had further discussions about the problems of synchronization, QoS, path optimization, and security. The authors [13] also stated that the evolution of new technologies shows how the size and management ability of the backhaul gadgets are directly affected by that throughput. The problems of synchronization encountered at the operation of LTE in a time-division duplex mode and subsequent evaluation of the solutions, such as synchronous Ethernet based on ITU standard G.8261 and accurate time protocol based on 1588v2, are discussed in detail [14].

C-RAN and its architecture were provided with an advanced solution by the author [15]. CRAN yielding, like system enhancement, the performance of coverage, movement, curbing utilization, and running cost. Along with the emphasis on ultra-dense mobile networks and mm Wave communication services, the latency and energy efficiency of 5G wireless gigabit networks were stated. The upcoming challenges of 5G and small cells were also discussed while adopting it. The authors also demonstrated the direct influence of ultra-dense small cells on the backhaul gateway [16]. Furthermore, the conclusion was reached that a more cooperative base station group is essential for the 5 G-based handoffs for outstanding gigabit results.

The security aspects in ITU-T X.805 stimulate the idea of the security control class, and ISO and NIST locate the security controls in security standards [17]. Providing a breakdown of the essential security operations and security concerns like privacy, accessibility, security, and authentication is the rationale behind the security control classes. The considered domain, layer, or security realm is required for precise controls.

Proposed Methodology

5G, the latest generation of cellular networks, is the new evolution in the research arena and has recently gained prominence as a promising idea in the technical field across the

DOI: https://doi.org/XXXX.XXXX

world. In the past three years, many research articles have been produced regarding it. A holistic view of 5G security, in general, is presented in this section and later throws light on the security problems of the physical layer and solutions as shown in **Fig. 1.** Creating a baseline integrated security standard for all slices is proposed to protect these, in addition to application-specific security for distinct slices. Eavesdropping is entirely protected by LTE [18] radio access; however, it is contrary to modifications or data boosters that are deemed the latest security concerns in cellular networks. Security against DoS, cloud security, and the latest trust models for managing unruly objects, weightless encryption solutions for power-sensitive objects are various other concerns. It is inferred that the latest Information Technologies [19], for example, SDN and NFN, along with other IoT, could increase DoS attacks [20]. The utilization of decentralized authentication is the alternative remedy. Unlike the centralized authentication servers, this signifies no single failure. The shortening distances are also permitted by it, which means till the end of the network, the server that can be shifted would also be conducive for the asymmetric key management system [21]. Amid the User Equipment and egress gateways on the operators' networks, the back-to-back user plane protection moves. Hence, the curbing of transmission distances could be carried out by moving the egress gateways from the center point to the edge [22].

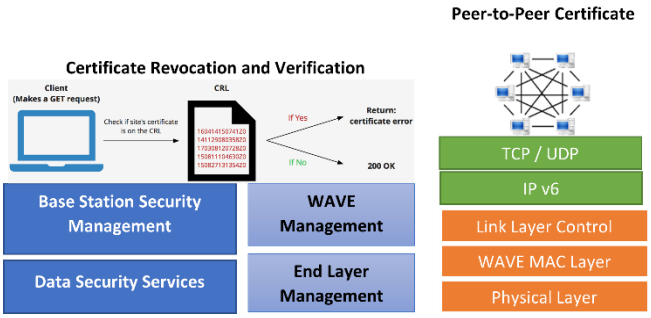


Fig. 1. IEEE WAVE Network Architecture

I. Fully Automated Attack Detection Model

Research on 5G security can be done to prevent attacks, depending on the hierarchical attack detection model. However, the possession of domain knowledge and manual interventions is required in many 5G security-related research types that are tough to meet the security needs related to the accuracy, coverage, and punctuality of privacy issues [23]. Hence, to solve the security problems of 5G, automated attack detection has turned out to be the primary research. An automated attack detection structure for 5G networks has been proposed in this section. 5G automated attack detection contains four parts: automated attack detection technologies, data related to security matters, and the security testbed [24]. **Fig. 2**. shows the automated attack detection structure. 5G networks' massive security data is the basis of a 5G security knowledge graph built first. The automated attack detection technologies are backed up by building a hierarchically directed graph using the knowledge graph. The results can be fed back to the knowledge graph by analyzing automated attack technology for locating the current and potential security issues. Finally, the verification platform can be created to the latest automated attack detection techniques by analyzing the security testbed [25].

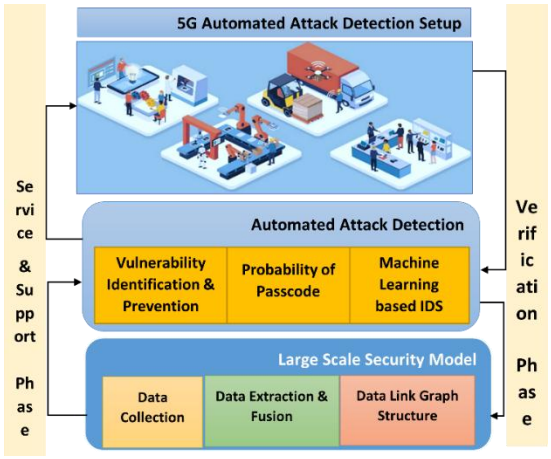


Fig. 2. Framework for Autonomous Detection of Attacks

A. Automated Attack Method

The following is the study conducted on automated attack detection: (1) key automated attack technologies, including guessing passwords, automated attacks based on Artificial Intelligence (AI), automated vulnerability exploitation and mining, etc. (2) To find the current attack chains and potential attack chains, we use the attack chain search and generation technology by merging the key automated attack technologies on the graph directed hierarchical [26]. This merging results in an integrated automated attack detection method. The automatic finding of vulnerabilities from software/protocols is performed by automated vulnerability mining technology. The automatic location of the return address and layout memory for implementing vulnerability information-based shellcode will be executed by the automated vulnerability exploiting technology [27]. To bypass security detection, the automated attack based on AI is constantly used; for example, by modifying the character and device access rule with AI technology, the security detection of the DoS attack on the Base Station can be bypassed. The study of current attack chains' features leads to the finding of potential attack chains using AI technology. Utilizing the above technologies on key automated attack detection and security knowledge graphs enhances the finding of specific attack methods for each edge of the potential attack chain [28].

B. User Authentication and Authorization Control

In addition to real-time control, the services also provide automotive machine vision to investigate the quality needs of fully automated machine learning, bandwidth efficiency, crane remote control, and UAV transportation. It is assumed that if data transmission is impossible outside the campus, then a large campus coverage area is redundant, and more security requirements are warranted [29]. There is a deployment of the User Plane Function and Multiaccess Edge Computing at the local edge, besides isolation of various service networks **Fig. 3.**

DOI: https://doi.org/XXXX.XXXX

This is the body text with an indent. This is the body text with an indent. This is the body text with an indent. This is the body text with an indent. This is the body text with an indent. This is the body text with an indent. This is the body text with an indent. This is the body text with an indent. This is the body text with an indent. This is the body text with an indent.

Secondly, for providing terminals that could access the slice in Username and Password mode with secondary authentication, the authentication and authorization systems in the security service zone are deployed by enterprises [30]. Terminals and applications with high-security needs enhance secondary authentication strength through authentication and Authorization systems and secure wireless technology. Here, the USIM-based security wireless card has an in-built USB key function that depends on the Public Key certificate system [31]. The wireless security chip stores the key, and hence copying, disclaiming, or tampering with it is impossible. Thirdly, the Multiservice Access Gateway can be deployed by the enterprise at the intranet border. The private enterprise network grants the terminals access rights to the private enterprise network by the Multiservice Access Gateway once the terminals pass the second authentication [32].

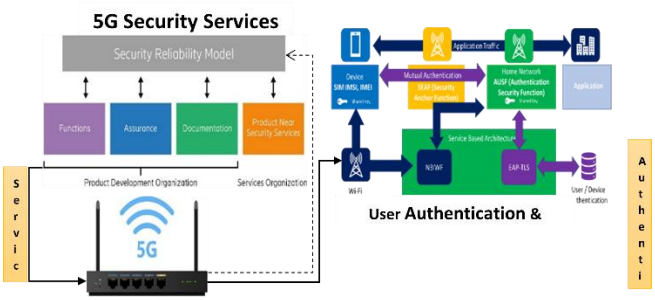


Fig. 3. Control of Advanced User Access

C. Literature survey

The most crucial part of the automated attack detection model is the 5G testbed. The verification of the latest security technologies can be done on the testbed for one reason. For another reason, despite the deployment of a 5G network, the performance of an attack experiment on the actual network is not feasible [33]. The intensive study of the existing security threats can be done based on the testbed, and the detection of potential security threats materialized and efficiently answered. At present, distinct testbeds for 5G networks are proposed; however, there is a lack of test cases for 5G security, particularly for automatic attack research [34]. The 5G security test case can be investigated in two dimensions: (1) For huge-scale, adaptable, and actual security testing, an integrated testbed framework can be constructed. The implementation of simulation can be gradually done based on the integrated testbed framework [35]. (2) The security research on the identical layer can be performed by investigating an exclusive security testbed of a layer, like the realistic layer security testbed and the virtual layer security test case. The testbed should also consider the association of security with the remaining layers. (3) A study can be conducted on the testbed for vertical services. The testbed enables simulation and reproduction of security situations for a particular service, for example, the smart city, smart premises, etc., as distinct services and applications are provided by the 5G network [36].

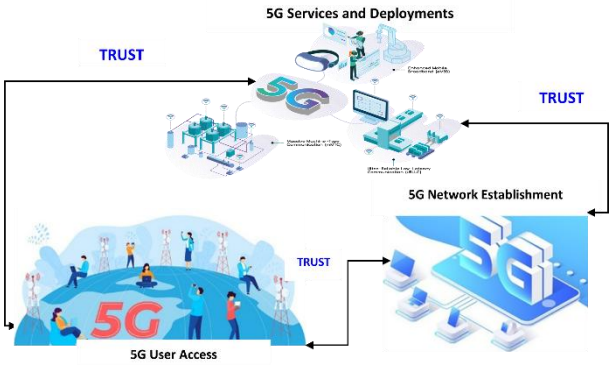


Fig. 4. Model of 5G Trust vs. 4G Network

In order to make network slicing effective, this concept is introduced in 5G for slicing the network for various applications and roles. Slicing is the optimum solution since the input or the data emerges from distinct resources, and the data type is distinct [37]. The isolated sub-networks provided by slicing can be enhanced for a particular kind. Slicing confines, the effect of security needs on a unified slice is supported by the accurate execution of the high assurance mechanism. This is an alternative way for security services enhanced by the network, resulting in attracting multiple user groups [38]. The above classes include network infrastructure security policies and procedures, access control key management, and cybersecurity services. The trust model in 5G is given in **Fig. 4.** It is evident that the user and network rely on one another in 4G, and the required service is applied and possesses encryption and a cybersecurity system, which secures the information. As we can see, the 5G trust model provides service on demand. The reliability exists between the user and network in the 5G trust model because the system is encrypted, and the user covers the vulnerabilities. The need or demand for service by the user relies on both the ways of requesting and receiving [39].

Results and discussion

The research queries asked at the initial stage of this report are given using the intellect earned from the literature study in this chapter.

A. Research Question-I

Which characteristics of 5G NR can be used for enhancing security at the realistic layer? Could there be any simplification or total removal of security mechanisms from higher-layer protocols?

Research Solution-I

The new security potentials to be introduced with 5G for three selected use cases are analyzed. Collision risk warning and decentralized floating car data, and Emergency vehicle warning are the above three cases. As an exclusive type of vehicle sends the message, the first case is fascinating. Since various users and

DOI: https://doi.org/XXXX.XXXX

RSUs send Collision risk warnings, it seems interesting. Ultimately, due to the creation of accessibility risks by the Decentralized floating described already, car data is quite interesting. At last, a discussion on the redundant cryptographic mechanisms is conducted.

Regarding the study, in all three cases, integrity is required, and the receivers primarily require authentication as far as the sender's location is concerned (other than the Emergency vehicle warning situation, where there is a requirement of accurate identity authentication). Simultaneously, for tracking misbehaving users persistently, the authorities wanted the identity.

(i) Integrity: Physical layer integrity is also enabled in the physical layer authentication implementation. To comprehend this, assume the situation where an attacker needs to change a message, i.e., attack message integrity. In such a situation, first, the attacker needs to intercept the message, then change it, and lastly, redirect it to the endpoint. The disclosure of the attacker's location will be inappropriate to the sender's anticipated location, assuming that physical layer authentication is used. This reveals that the anticipated user did not send the message since there has been an attack.

(ii) Accessibility: All three cases and indeed all the road safety-critical use cases, in general, require accessibility. The Decentralized floating car data indicate a specific accessibility risk. An attacker might enormously provoke such "waves" messages as the use case messages are reiterated from one car to another (spreading the warning over a greater distance. An outpouring of the message, which clogs the network, is the potential outcome, and it hinders legal users from accessing the network. In order to evade this sort of attack, it is essential to propose security mechanisms. The deployment of NOMA scheduling and cognitive radio networks facilitates better accessibility.

(iii) Confidentiality: Since road safety messages do not transmit any sensitive user data, it is unproblematic in those situations anyway. Indeed, this is possibly the cause for CAMs and DENMs (ITS) security profile, to mention that there is no encryption of these messages. However, it is observed that confidentiality is, in fact, significant in some use cases. For example, in the Automatic access control/parking management use case.

B. Research Question-II

Which characteristics of 5G NR can be used for enhancing security at the realistic layer? Could there be any simplification or total removal of security mechanisms from higher-layer protocols?

Research Solution-II

Whether the smooth replacement of 802.11p with 5G NR is feasible or not is one of the research questions asked initially. Because NR is not yet determined and could hence be enhanced as per requirement, the brief answer is 'Yes'. The modification of transmission frequencies or an alternative scheduling method (NOMA) should not influence the higher-layer protocols because of the network stack's modularity, as shown in **Tab. 1.**

Tab. 1. Strengths and Weaknesses of 5G

Strengths	Weakness
When the input load increases, i.e., in metropolitan areas, it becomes more reliable.	Highly restrictive synchronization performance standards
A network is set up for scheduling and load balancing (more minor collisions)	Worse at dealing with collisions
The global network explains the problem of hidden nodes.	The primary issue of near-far is proposed
More adaptable utilization of resources	Transmitted signal susceptible
wider range coverage	Less suitable to out-of-coverage circumstances

Conclusions

Social life and vertical industries have a profound incorporation of 5G. The application developers and service providers and equipment suppliers, and network operators predominantly affect the 5G ecosystem's security and privacy. The overall security factors from wireless devices, Wi-Fi networks, edges, and other issues besides typical usage scenarios' specific risks are analysed in this paper. In this connection, a broad background of past and existing networks, contrary to the future 5G, is furnished. Enhancement of the QoS parameter is the predominant idea of this study, and therefore, after implementing 5G mobile communications in 2025, those will have a primary focus. There is an assimilation of physical layer security and logical layer security in this paper, and with the perception of automated attack detection, 5G security is investigated. Numerous researchers and industry-oriented people predict that 5G is the upcoming technology for Vehicle-to-Everything communications because of the novelties in speed and other technological inventions in 5 G. As a result, the profound study of 5G security and its incorporation into the existing ITS model is warranted. Ultimately, an industrial terminal access control's use case in which understanding particular 5G application security risks and solutions by the readers is enhanced. This article thoroughly investigates security and privacy in 5G applications that reinforce awareness of risk and potential of security and positively impact the wholesome and enduring enhancement of several applications in the 5G era.

References:

DOI: https://doi.org/XXXX.XXXX

[1] O. I. Khalaf, G. M. Abdulsahib, .H. D. Kasmaei, & K. A. Ogudo, “A new algorithm on application of blockchain technology in live stream video transmissions and telecommunications”. International Journal of e-Collaboration (IJeC), 16(1), 16-32, (2020).

[2] A. D. Salman1, O. I. Khalaf and G. M. Abdulsahib, “An adaptive intelligent alarm system for wireless sensor network”. Indonesian Journal of Electrical Engineering and Computer Science, Vol. 15, No. 1, July 2019, pp. 142~147.

[3] N. Sulaiman, G. Abdulsahib, O. Khalaf, M. N. Mohammed, "Effect of Using Different Propagations of OLSR and DSDV Routing Protocols", Proceedings of the IEEE International Conference on Intelligent Systems Structureing and Simulation, pp. 540-545, 2.

[4] R. Sardar *et al.*, “Challenges in detecting security threats in WoT: a systematic literature review,” *Artif Intell Rev*, vol. 58, no. 7, 2025, doi: 10.1007/s10462-025-11176-z.

[5] A. Asasfeh, N. A. Al-Dmour, H. Al Hamadi, W. Mansoor, and T. M. Ghazal, “Exploring Cyber Investigators: An In-Depth Examination of the Field of Digital Forensics,” in *2023 IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Tec*, 2023, pp. 84–88. doi: 10.1109/DASC/PiCom/CBDCom/Cy59711.2023.10361449.

[6] A. Arabiat and M. Altayeb, “Enhancing internet of things security: evaluating machine learning classifiers for attack prediction,” *International Journal of Electrical and Computer Engineering*, vol. 14, no. 5, pp. 6036–6046, 2024, doi: 10.11591/ijece.v14i5.pp6036-6046.

[7] K. S. Pokkuluri, A. Kumar, K. K. S. Gautam, P. Deshmukh, G. Pavithra, and L. Abualigah, “Collaborative Intelligence for IoT: Decentralized Net security and confidentiality,” *Journal of Intelligent Systems and Internet of Things*, vol. 13, no. 2, pp. 202–211, 2024, doi: 10.54216/JISIoT.130216.

[8] A. Qaddos, M. U. Yaseen, A. S. Al-Shamayleh, M. Imran, A. Akhunzada, and S. Z. Alharthi, “A novel intrusion detection framework for optimizing IoT security,” *Sci Rep*, vol. 14, no. 1, 2024, doi: 10.1038/s41598-024-72049-z.

[9] M. Maaz, G. Ahmed, A. S. Al-Shamayleh, A. Akhunzada, S. Siddiqui, and A. H. Al-Ghushami, “Empowering IoT Resilience: Hybrid Deep Learning Techniques for Enhanced Security,” *IEEE Access*, vol. 12, pp. 180597–180618, 2024, doi: 10.1109/ACCESS.2024.3482005.

[10] M. W. A. Ashraf, A. R. Singh, A. Pandian, M. Bajaj, I. Zaitsev, and R. S. Rathore, “Enhancing network security with hybrid feedback systems in chaotic optical communication,” *Sci Rep*, vol. 14, no. 1, 2024, doi: 10.1038/s41598-024-76391-0.

[11] B. M. Elomda, T. A. A. Abdelbary, H. A. Hassan, K. S. Hamza, and Q. Kharma, “An Enhanced Multi-Layer Blockchain Security Model for Improved Latency and Scalability,” *Information (Switzerland)*, vol. 16, no. 3, 2025, doi: 10.3390/info16030241.

[12] T. M. Ghazal, M. K. Hasan, H. M. Alzoubi, M. Alshurideh, M. Ahmad, and S. S. Akbar, *Internet of Things Connected Wireless Sensor Networks for Smart Cities*, vol. 1056. 2023. doi: 10.1007/978-3-031-12382-5_107.

[13] L. Almahadeen *et al.*, “Enhancing Threat Detection in Financial Cyber Security Through Auto Encoder-MLP Hybrid Models,” *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 4, pp. 924–933, 2024, doi: 10.14569/IJACSA.2024.0150495.

[14] J. V. N. Ramesh *et al.*, “Satellite IOT Terminal Authentication Mechanism for Enhancing Consumer Security Over Cyber-Physical Systems,” *IEEE Transactions on Consumer Electronics*, 2025, doi: 10.1109/TCE.2025.3535078.

[15] Y. Sanjalawe, S. Al-E’mari, S. Fraihat, M. Abualhaj, and E. Alzubi, “A deep learning-driven multi-layered steganographic approach for enhanced data security,” *Sci Rep*, vol. 15, no. 1, 2025, doi: 10.1038/s41598-025-89189-5.

[16] U. S. Kumar *et al.*, “Fusion of MobileNet and GRU: Enhancing Remote Sensing Applications for Sustainable Agriculture and Food Security,” *Remote Sens Earth Syst Sci*, vol. 8, no. 1, pp. 118–131, 2024, doi: 10.1007/s41976-024-00183-3.

[17] Y. Aldaaja *et al.*, “Quantifying the Managerial and Practical Benefits of Cloud Computing on Information Security in Higher Education Institutions,” *Applied Mathematics and Information Sciences*, vol. 19, no. 1, pp. 15–24, 2025, doi: 10.18576/amis/190102.

[18] Y. Hassan *et al.*, “Exploring the Mediating Role of Information Security Culture in Enhancing Sustainable Practices Through Integrated Systems Infrastructure,” *Sustainability (Switzerland)*, vol. 17, no. 2, 2025, doi: 10.3390/su17020687.

[19] A. Mughaid, I. Obeidat, L. Abualigah, S. Alzubi, M. S. Daoud, and H. Migdady, “Intelligent cybersecurity approach for data protection in cloud computing based Internet of Things,” *Int J Inf Secur*, vol. 23, no. 3, pp. 2123–2137, 2024, doi: 10.1007/s10207-024-00832-0.

[20] R. Al-Sayyed, E. Alhenawi, H. Alazzam, A. Wrikat, and D. Suleiman, “Mobile money fraud detection using data analysis and visualization techniques,” *Multimed Tools Appl*, vol. 83, no. 6, pp. 17093–17108, 2024, doi: 10.1007/s11042-023-16068-4.

[21] S. Tumula *et al.*, “An enhanced bio-inspired energy-efficient localization routing for mobile wireless sensor network,” *International Journal of Communication Systems*, vol. 37, no. 12, 2024, doi: 10.1002/dac.5803.

[22] T. M. Ghazal et al., Machine Learning-Based Intrusion Detection Approaches for Secured Internet of Things, vol. 1056. 2023. doi: 10.1007/978-3-031-12382-5_110.

[23] A. Al Sharah, Y. A. Alrub, H. A. Owida, E. A. Elsoud, N. Alshdaifat, and H. Khtatnaha, “An Adaptive Framework for Classification and Detection of Android Malware,” *International Journal of Interactive Mobile Technologies* , vol. 18, no. 21, pp. 59–73, 2024, doi: 10.3991/ijim.v18i21.49669.

[24] A. A. Althuwayb *et al.*, “Multi antenna structure assisted by metasurface concept providing circular polarization for 5G millimeter wave applications,” *Sci Rep*, vol. 15, no. 1, 2025, doi: 10.1038/s41598-025-02208-3.

[25] R. I. Al-Suhimat et al., "Review of Security Challenges Encountered in Internet of Things Technology," in *Proc. 2nd Int. Conf. Cyber Resilience (ICCR 2024)*, Dubai, UAE, 26–28 Feb. 2024, doi: 10.1109/ICCR61006.2024.10533052.

[26] M. K. Hasan et al.,"Towards Privacy Provisioning for Internet of Things (IoT)," in *Proc. 2022 Int. Conf. Cyber Resilience (ICCR 2022)*, doi: 10.1109/ICCR56254.2022.9995916.

[27] A. Sharma, K. J. Singh, D. S. Kapoor, K. Thakur, and S. Mahajan, *Advancements in 5G-IoT Technology-Based Healthcare: A Focus on Healthcare Monitoring for Smart Cities*, vol. Part F4006. 2025. doi: 10.1007/978-3-031-72732-0_5.

DOI: https://doi.org/XXXX.XXXX

[28] M. H. Ali et al.,"xdata for transmission in wireless communication networks," *Periodicals of Engineering and Natural Sciences*, vol. 9, no. 4, pp. 1038–1055, 2021, doi: 10.21533/pen.v9i4.2570.

[29] M. H. G. Muhammad et al., "Resource Provisioning in Cloud Computing using Fuzzy Logic Control System: An Adaptive Approach," in *Proc. 2nd Int. Conf. Business Analytics for Technology and Security (ICBATS 2023)*, Dubai, UAE, 7–8 Mar. 2023, doi: 10.1109/ICBATS57792.2023.10111481.

[30] M. A. Aljubouri and M. Z. Iskandarani, "Comparative analysis of coding schemes for effective wireless communication," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 34, no. 2, pp. 926–940, 2024, doi: 10.11591/IJEECS.V34.I2.PP936-950.

[31] M. Z. Iskandarani, "Communication Analysis of Wireless Sensor Networks with Mobility Function," in *International Conference on Electrical, Computer, Communications and Mechatronics Engineering, ICECCME 2024*, 2024. doi: 10.1109/ICECCME62383.2024.10796204.

[32] M. Otair *et al.*, "Enhanced Arithmetic Optimization Algorithm for Intrusion Detection in Wireless Sensor Networks," *International Journal of Communication Systems*, vol. 38, no. 10, 2025, doi: 10.1002/dac.70122.

[33] E. Anaam, M. K. Hasan, T. M. Ghazal, S. C. Haw, H. M. Alzoubi, and M. T. Alshurideh, "How Private Blockchain Technology Secure IoT Data Record," in *2023 IEEE 2nd International Conference on AI in Cybersecurity, ICAIC 2023*, 2023. doi: 10.1109/ICAIC57335.2023.10044178.

[34] G. Kiran Kumar *et al.*, "An optimized meta-heuristic clustering-based routing scheme for secured wireless sensor networks," *International Journal of Communication Systems*, vol. 37, no. 11, 2024, doi: 10.1002/dac.5791.

[35] L. Abualigah *et al.*, "Optimizing Intrusion Detection in Wireless Sensor Networks via the Improved Chameleon Swarm Algorithm for Feature Selection," *IET Communications*, vol. 19, no. 1, 2025, doi: 10.1049/cmu2.70029.

[36] N. C. Masango *et al.*, "Secure and efficient cloudlet networks: blockchain integration with agent-based proof of trust mechanism," *EURASIP J Wirel Commun Netw*, vol. 2025, no. 1, 2025, doi: 10.1186/s13638-025-02439-y.

[37] A. S. Mohammed et al., "Unveiling the Landscape of Machine Learning and Deep Learning Methodologies in Network Security: A Comprehensive Literature Review," in *Proc. 2nd Int. Conf. Cyber Resilience (ICCR 2024)*, Dubai, UAE, 26–28 Feb. 2024, doi: 10.1109/ICCR61006.2024.10533066.

[38] R. Sekhar et al.,"Security and Privacy Protection for Online Electronic Documents Based on Novel Encryption Techniques," *J. Intell. Syst. Internet Things*, vol. 11, no. 1, pp. 21–28, 2024, doi: 10.54216/JISIoT.110103.

[39] A. Ibrahim, "Guarding the Future of Gaming: The Imperative of Cybersecurity," in *Proc. 2nd Int. Conf. Cyber Resilience (ICCR 2024)*, Dubai, UAE, 26–28 Feb. 2024, ISBN 979-835039496-2, doi: 10.1109/ICCR61006.2024.10532843.

DOI: https://doi.org/XXXX.XXXX