

Analysis of Modern Approaches to Security in IoT Networks

Marieta Haka

Technical University of Varna/ Faculty of Computer Sciences and Automation, Varna, Bulgaria

marieta.yordanova@tu-varna.bg

Abstract: IoT networks pose many security challenges due to the transfer and storage of a large amount of data and the need for a long battery life of the end devices. Cyberattacks on IoT devices are growing daily and detecting them and limiting their consequences is key to consumer trust in IoT-based solutions, and hence their wider application in various business solutions. This article presents an analysis of the advantages and disadvantages of approaches to increasing security in IoT networks based on blockchain technologies, artificial intelligence and cryptographic security methods.

Keywords: IoT, Security, Blockchain, Artificial Intelligence, Cryptographic Solutions.

Received 26 September 2024

Accepted 30 November 2024

Published 20 December 2024

1. Introduction

Internet of Things (IoT) is a technology that allows connected objects on a network such as software applications and intelligent systems to interact, collect, and process massive amounts of data, providing a variety of services to end users. IoT devices range from small sensors and actuators to smart tools, enabling companies to automate processes and reduce labor costs in healthcare, smart home, and smart industry with multiple applications [1].

Over the past 5 years, IoT has had a significant impact on the advancement of communication by enabling the integration of disparate objects within a unified network. Thanks to this technology, companies can automate processes and reduce labor costs. IoT is one of the most important technologies for business and everyday life and has the potential to gain momentum in usage [2]. The number of IoT devices is expected to exceed 29 billion by 2030, indicating the rapid growth of IoT [3]. In recent years, IoT data transmission has been increasing due to the integration of IoT applications across a wide range of domains [4].

IoT applications are being integrated across a wide range of industries, leading to the rapid expansion of the market. Wireless Sensor Networks (WSNs) play a critical role in IoT deployment [5]. In addition, WSN is an essential technology especially for real-time application development. They enable automation of various processes based on measured environmental parameters. WSN is used in healthcare and other industries to transform various service sectors that use IoT data transmission [2].

Despite the benefits of IoT, cyber-attacks are becoming more frequent as the flow of IoT data increases, posing a

threat to the privacy of IoT data. The limited processing power and insufficient memory resources of IoT devices make it difficult to implement comprehensive security mechanisms. Because of these limitations, devices are vulnerable to attacks that allow unauthorized access to private information [6]. As a result, devices are susceptible to attacks such as BotNet, Man-in-the-middle, Distributed Denial of Service (DDoS) [7,8]. Due to these vulnerabilities, it is crucial to ensure the security of IoT communication sessions. Identifying resource-constrained devices and their associated resources is a challenging task in today's busy environment [9].

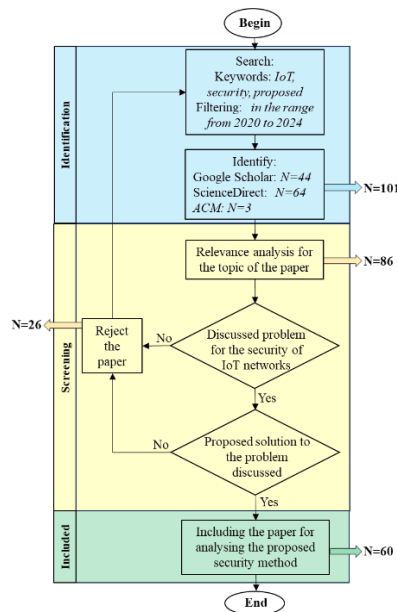
The process for recruiting research papers is performed systematized according to the algorithm shown in Figure 1, following the main steps of the updated PRISMA method [10]. During the review of papers, a search is made for the keywords "IoT", "security" and "proposed" in the databases of Google Scholar, Science Direct and ACM.

The search is filtered in the range from 2020 to 2024. As a result, a total of 101 research papers are identified. The purpose of this filtering is to find contemporary paper related to the topic. After analyzing the papers for relevance through their abstracts, 86 scientific of them are identified. Then, an analysis is made of whether the problem related to IoT security is discussed and whether a solution to this problem is proposed. The papers that do not comply these criteria are 26 and are thus not considered. The residual 60 papers are considered the most proper for analyzing modern approaches to secure IoT networks.

2. IoT Security Technologies

Various technologies such as Blockchain, Artificial Intelligence, and Cryptographic methods are being used to ensure the security of IoT which have been improving the security of IoT over the last 5 years. These technologies are an integrated approach to protect devices and their data from various types of cyber-attacks. Combining them into a holistic approach is essential to create resilient and secure IoT systems in the future.





improve access management, protect data from hacking attacks and ensure secure communication between IoT devices.

Despite these advantages, the application of Blockchain solutions to IoT security causes a scalability problem because Blockchain networks create difficulties in managing the large amount of data generated by IoT devices, which can lead to difficulties in managing large volumes of data and delays in processing [23]. The complexity of integration and lack of standardization increase the cost and challenges of deploying IoT ecosystems that use Blockchain methods [24].

2.2. Artificial intelligence

Artificial intelligence methods also have an important role to play in improving IoT security. AI-based cyber-attack detection and prevention systems can identify anomalies and potential threats, enabling a fast and effective response to potential incidents.

In [25], an automatic intrusion detection system is proposed using a well-known machine learning model, Random Forest, on a dataset (UNSW-NB15). The goal of this proposal is to improve the detection rate and reduce false problem alerts by improving the detection accuracy of network attacks. In [26], a CyberAIBot intrusion detection system for IoT cybersecurity targeting operational and information technology network traffic is presented. The proposed solution in [27] includes a cost-based classifier (CRFC) to develop an efficient Intrusion Detection System (IDS). The CRFC based classification is improved by incorporating a cost matrix computed based on feature importance which helps to improve the feature separation process even if there is feature imbalance.

In [28], an efficient IoT network anomaly mitigation system is developed by designing and deploying a DDoS attack detection system that uses a statistical method combining three algorithms: exponentially weighted moving average (EWMA), K-nearest neighbors (KNN), and cumulative sum (CUSUM) algorithm. In [29], an IoT-driven cross-device method is proposed to learn an IDS model on the traffic of different IoT devices included in the widely used N-BaIoT dataset. The purpose of this method is BotNet discovery from IoT through Deep Autoencoders. In [30], a feature selection solution is proposed using a classifier based on genetic algorithm. The aim of the method is intrusion detection in the IoT environment which is facing threats from BotNet attacks. The research [31] presents an approach to reduce DDoS attacks by being closer to the source of the attack, which provides faster response and greater efficiency. This approach combines host-based and network-based intrusion detection systems (HIDS and NIDS). The model offers a blended approach to anomaly detection at both the local and network level. The use of federated learning allows devices to process their data locally and contribute to the overall detection system, which improves the accuracy of detected anomalies and reduces the load on centralized systems.

In the research [32], a flexible edge (Edge) security approach is created that automatically creates and adapts security policies for edge IoT devices. The approach combines a dynamic security policy generator with a

conflict detection and resolution system, a bias-aware risk assessment system, a regulatory compliance analysis system, and an AI-driven adaptivity integration system. In [33], a Blockchain based security system is proposed that uses PUF model to protect IoT devices by sharing alarm signals in the network. The use of machine learning and Blockchain technology results in low false positive rates and high detection accuracy in the system. The goal of this model is to efficiently and securely share data across the network, which reduces the likelihood of cyber-attacks and improves the overall security of IoT infrastructures. In [34], critical security challenges on the Internet of Things (IoT) domain are addressed by applying a solution that combines Convolutional Neural Networks (CNN) for feature extraction and the XGBoost model for intrusion detection. By applying the introduced hyperparameter optimization algorithm, more efficient models capable of handling intrusion detection effectively are constructed.

In [35], a complete real-time cyber-attack detection architecture is developed to simulate complex attack scenarios and provide appropriate countermeasures. The architecture uses current data and artificial intelligence modules to analyze and visualize threats, which improves the understanding of attacks and response capabilities. The goal of this system is to analyze data and prevent cyberattacks in a virtual environment, which is key to verifying and validating various defense methods.

Artificial Intelligence solutions enable proactive detection of new and unknown threats by analyzing network traffic anomalies. They can continuously learn and adapt to new types of attacks, such as DDoS or BotNet, and identify complex patterns of behavior in real time.

Despite these advantages, using artificial intelligence to protect IoT has several drawbacks. Using AI systems can be costly and difficult to deploy, especially for small businesses, and increases the potential for cyberattacks by creating new risks. Also, AI can create false positives, making it more difficult to detect new threats. This creates vulnerability to new cyber-attacks [36]. Such solutions often require a large amount of data and computational resources for training and analysis, which can be challenging for IoT devices with limited resources [37].

2.3. Cryptographic methods

Cryptographic methods are essential for securing IoT networks. Technology encompasses various methods such as symmetric and asymmetric encryption and hashing that protect communication and information from unauthorized access and manipulation, ensuring data confidentiality and integrity. The use of cryptographic techniques enhances the protection of communication channels, data generated by IoT devices, and the management of these devices [38]. Protecting data privacy in IoT settings is critical, as exposure of sensitive data can lead to challenges for both organizations and individuals. There is research addressing this problem by applying cryptographic techniques [39]. The proposal presented in [40] involves using a combination of end-to-end encrypted messages to solve the problem. To protect the useful data generated by MQTT, the Fernet cryptographic method is applied. This method provides authentication using SHA256 for hashing and AES128 for encryption

algorithms. The study in [41] presents an innovative algorithm that uses artificial intelligence to improve the encryption process of autonomous IoT systems. The main goal of the algorithm is to minimize the computational complexity associated with data encryption at both endpoints and intermediate nodes of IoT systems. To achieve this, an MD5 hashing algorithm is used on the encrypted data collected in IoT. The proposal in [42], involves the development and implementation of a cryptographic system for IoT. The system uses the AES algorithm in Electronic Code Book, Cipher Block Chaining and Counter modes of operation as well as additional security schemes such as AES Galois/Counter Mode and AES Galois Message Authentication Code to encrypt and decrypt text, images and electronic data applications. The research in [43] introduces adaptive eXtensible Access Control Markup Language (XACML) access policies specifically designed for heterogeneous distributed IoT environments. The main goal of these policies is to extend the capabilities of traditional XACML by integrating access code generation and verification schemes. To ensure the security of the access code, it is encrypted using MD5 and SHA-1 hashing. In [44], an algorithm is presented that uses artificial intelligence to improve the encryption process of autonomous IoT systems. The main goal of the algorithm is to minimize the computational complexity associated with data encryption at both endpoints and intermediate nodes of IoT systems. To achieve this, the algorithm uses MD5 hashing to encrypt the data collected at the IoT end nodes.

In [45], Lamport Merkle Digital Signature Verification is implemented to protect sensitive patient data from unauthorized access. Furthermore, authentication of IoT devices is achieved by creating hash value trees using Lamport Merkle Digital Signature. The goal of this strategy is to increase the security and privacy of IoT devices used in healthcare. In [46], the challenges associated with the identification and authentication of IoT devices are addressed by proposing the Secure Communication and Authentication for IoT applications using the Blockchain method. Using Blockchain and a hybrid cryptosystem that includes AES, the Elliptic Curve Digital Signature Algorithm (ECDSA) and the SHA hash function, this method provides a complete security solution. AES is used to ensure the confidentiality of communication between two devices, while ECDSA establishes secure communication between the device and the cluster coordinator. The goal of this approach is to strengthen IoT security measures by providing protection against potential attacks and optimizing computation and storage costs.

In [47], an architecture for AES that is resilient to errors and attacks is proposed for IoT applications, offering a cost-effective solution for error detection in security applications. By integrating the processes of AES encryption and decryption, it provides a comprehensive approach to real-time data protection. The architecture allows for efficient processing and ensures that the system can detect and handle errors. The study in [48] presents a scheme for preserving the privacy of data generated by IoT devices. The scheme proposes the use of homomorphic encryption to protect the data sent from user devices to the

coordinator. By employing this encryption technique, the scheme aims to prevent unauthorized access and ensure that unreliable cloud servers cannot obtain information about the specific tasks performed on the patient's encrypted data.

The main objective is to enhance the confidentiality and security of sensitive medical information, thereby instilling confidence in patients and healthcare providers regarding the protection of their data. A scheme for authenticated key agreement is proposed in [49]. By utilizing Elliptic Curve Cryptography (ECC), the proposed solution ensures a high level of protection against unauthorized access. This approach guarantees the maintenance of trust and reliability of IoT systems in the face of evolving cyber threats. The aim of the research in [50] is to ensure that users can search for specific information in Blockchain without compromising the security and integrity of the data. By integrating deep learning algorithms and homomorphic encryption, the system offers a reliable solution for protecting sensitive information while enabling effective searching. In [51], through a combination of different cryptographic algorithms, the proposed Hybrid and Adaptive Cryptographic framework aims to increase the security and reliability of communication channels in IoT networks. The use of AES, RSA, and ECC algorithms in a hybrid manner provides a reliable and versatile approach to encryption, meeting the diverse communication requirements of IoT devices. The study in [52] focuses on increasing the security of communication between IoT and Blockchain by introducing an algorithm to generate a secure secret code. By including a secure secret code in the original message generated by IoT devices, the algorithm aims to ensure confidentiality and integrity of the transmitted data.

Using ECC to generate a hash of the secret code and message adds an extra layer of protection against unauthorized access. In addition, AES is used to protect all information using a single secret key. These keys are pre-generated and distributed to the targeted devices, allowing them to decrypt the encrypted data. In [53], the NTM-LEACH-RSA algorithm is used to solve security problems in WSN. The main objective of this approach is to optimize energy use while extending the uptime of the network. Using a cryptographic algorithm, RSA communication and data integrity within WSN are effectively protected. In [54] it is presented the development of Reconfigurable ASCON Hash Functions for IoT Applications (RECO-ASCON) - a reconfigurable cryptographic processor that offers a solution for working with multiple hash modes. By incorporating the ASCON Hash and Hasha algorithms, this solution provides secure message transmission in the IoT field. The versatility of RECO-ASCON allows it to adapt to different hashing requirements, providing a reliable cryptographic solution for IoT.

The main objective of [55] is to establish a reliable model for the protection of consumer data and the maintenance of the privacy of patients' personal data in the field of IoMT. To achieve this, a model for searching encrypted data and a hybrid cryptographic algorithm is employed, which combines the principles of the Caesar cipher, Elliptic Curve Diffie-Hellman (ECDH), and the

Digital Signature Algorithm (DSA). This combination enables the protection of messages during their transmission and facilitates secure key exchange between clients and healthcare centers. In [18], increasing the security and reliability of software updates is the main goal of the proposed Blockchain-based distributed software update framework. Using smart contracts and the ECDSA digital signature algorithm, the framework ensures the authenticity of the identity of the software creator. Additionally, the integrity of the software update is protected by verification using the SHA-3 cryptographic hash. This comprehensive approach aims to provide end-to-end protection and verification throughout the entire software delivery process.

In [56], to improve patient care and enable remote medical consultations, the MedIoTverse framework is presented. This framework covers vital parameters such as heart rate, blood pressure, and body temperature for effective patient monitoring. The focus of the proposed solution is to provide protection in the transmission of patient data to the health server. For this purpose, the AES-256 cryptographic algorithm is used, which provides a stable and reliable encryption method. The research in [57] aims to address vulnerabilities related to client IoT node authentication using the Tempered ECDSA algorithm. Using a timestamp that is not shared and has a short lifespan adds an extra layer of security to the authentication process. Cryptographic solutions are critical to the security of IoT networks, ensuring the

confidentiality, integrity, and authenticity of data, preventing unauthorized access and manipulation. Various methods such as AES, RSA, SHA-256, MD5, and ECDSA are used to encrypt, hash, and sign data, providing security when devices exchange information. Cryptographic algorithms such as AES and RSA provide secure communication and are reliable in critical systems where privacy is key. Also, solutions such as ECC and optimized versions of AES are suitable for resource-constrained devices in IoT, offering high security and minimal resource usage [58, 59].

Table 1 presents the most used IoT security methods. From the analysis of IoT protection, over the past 5 years, the most used methods are Blockchain and cryptographic approaches. Blockchain technology is used for its decentralized structure and high level of data protection through consensus mechanisms such as PoW, DPoS, and PBFT. However, generating a large volume of data from IoT devices can lead to processing delays, and this creates an inability to protect data. Cryptographic methods are used because of the ability to create high-security IoT solutions with minimal use of resources, which makes them preferred over Blockchain. Of the cryptographic methods considered, AES is the most used, as it is standardized by the National Institute of Standards and Technology in the United States [60] and is recognized as a secure and reliable cryptographic algorithm that is essential for the security of IoT networks [61].

Table 1. Existing IoT Security Solutions

	Technology	Method	References				
			2024	2023	2022	2021	2020
Security	Blockchain	Consensus Mechanisms	PoW	[11];	[20];		
			PoC			[21];	
			DPoS	[12];	[15];		
		Distributed Ledger	EOSIO	[12];			
			Hyperledger Fabric		[16]; [17];	[50];	
			Ethereum	[13];	[14]; [16];		
		Smart Contracts	[11]; [12]; [13];	[14]; [15]; [16]; [17]; [18];	[19]; [32]; [50];	[46]; [21];	
	(Artificial Intelligence)	IDS (Intrusion Detection System)	Support Vector Machines (SVM)	[24];		[32];	
			Random Forests (RF)	[26];			
			K-Nearest Neighbours (kNN)		[14]; [27];		
			Auto-encoders	[25];	[28];		[41];
			Recurrent Neural Network (RNN)	[34];		[50];	
			Genetic Algorithm (GA)		[29];		[44];
		IPS (Intrusion Prevention System)	Federated Learning		[31];		
			Convolutional Neural Networks (CNN)		[32];		
	Cryptographic solutions	Data Encryption	AES, RSA, ECC, DH	[9]; [55]; [58];	[17]; [48]; [51]; [31]; [49]; [52]; [50];	[45]; [46]; [47];	[41];
		Hash Functions	SHA256, MD5, SHA3	[10];	[15]; [17]; [51]; [53]; [54];	[40]; [42]; [43];	[39];
		Digital Signatures	RSA, ECDSA, DSA	[56];	[38]; [54];	[31];	[44]; [45];

1. Conclusion

This study examines the advantages and disadvantages of core security technologies in Internet of Object (IoT) systems, including blockchain, artificial intelligence, and cryptography. Blockchain improves access control and protects data from hacker attacks in the IoT but poses challenges with scalability and integration.

The lack of compliance with standards aggravates the costs and difficulties of using blockchain-based IoT systems. The capabilities of artificial intelligence include threat detection by analyzing atypical situations in network traffic, but its implementation comes with high costs and new risks, such as false alarms and the need for extensive data training. These factors could pose a serious problem for devices that have limited resources. Cryptographic methods are a mandatory component for securing IoT networks, ensuring the confidentiality, integrity, and authenticity of data. AES and RSA are efficient algorithms that provide secure communication and are used successfully in critical systems. Encryption methods are known for their minimal resource requirements, making them suitable for IoT devices with limited computing power. According to the study, the AES algorithm is the most used cryptographic method in IoT networks due to its efficiency and standardization. After the security techniques in IoT systems studied, the use of cryptographic methods for IoT security is mainly observed.

Their advantages such as offering high security with minimal resources make them suitable for environments with limited computing capabilities. Of the cryptographic methods, the use of the AES algorithm in IoT networks prevails. With key lengths of 128, 192, and 256 bits, this encryption algorithm is widely used due to its efficiency in making decryption a complex process.

References

- [1] Sayed, M. (2024). The internet of things (iot), applications and challenges: a comprehensive review., *Journal of Innovative Intelligent Computing and Emerging Technologies (JIICET)*, vol. 1, no. 01, pp. 20-27
- [2] Nassra, I. & Juan, V. (2023). Data compression techniques in IoT-enabled wireless body sensor networks: A systematic literature review and research trends for QoS improvement, *Internet of Things* vol. 23 pp.100806.
- [3] Eltayieb, N. Rashad E. Yongjian L. Fagen L. & Shijie Z. (2024). A heterogeneous signcryption scheme with Cryptographic Reverse Firewalls for IoT and its application" *Journal of Information Security and Applications*, vol. 83 pp.103763.
- [4] Garah, A. Nader, M. & Kirgizov, S. (2024). Enhancing IoT data confidentiality and energy efficiency through decision tree-based self-management, *Internet of Things* vol. 26 pp. 101219.
- [5] Liao, S. (2024). Blockchain Sensor Network Based CPS Analysis in Healthcare System for Real Time Applications Using 6G IoT Model and Deep Learning Techniques, *Wireless Personal Communications*, pp. 1-16, doi: 10.1007/s11277-024-11185-1
- [6] Rozlomii, I. Andrii, Y. & Serhii, N. (2024). Data security of IoT devices with limited resources: challenges and potential solutions, *In doors*, pp. 85-96.
- [7] Lokendra, V. & Das, D. (2021). SCAB-IoTA: Secure communication and authentication for IoT applications using blockchain, *Journal of Parallel and Distributed Computing*, vol. 154, pp. 94-105.
- [8] Ali, A. Pasha, M.F. Ali, J. Fang, O.H. Masud, M. Jurcut, A.D. Alzain, M.A. (2022). Deep Learning Based Homomorphic Secure Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography, *Sensors*, vol. 22, pp. 528, <https://doi.org/10.3390/s22020528>
- [9] Nadhan, A. S. & Jacob, I. J. (2024). Enhancing healthcare security in the digital era: Safeguarding medical images with lightweight cryptographic techniques in IoT healthcare applications, *Biomedical Signal Processing and Control*, vol. 88, pp.105511.
- [10] Ed-Dafali, S., Adardour, Z., Derj, A., Bami, A., & Hussainey, K. (2025). A PRISMA-Based Systematic Review on Economic, Social, and Governance Practices: Insights and Research Agenda, *Business Strategy and the Environment*, vol. 34, no.), pp.1896-1916.
- [11] Lin, Q. Li, X. Cai, K. Prakash, M., & Paulraj, D. (2024). Secure Internet of medical Things (IoMT) based on ECMQV-MAC authentication protocol and EKMC-SCP blockchain networking, *Information Sciences*, vol. 654, pp.119783.
- [12] Miao, J. Wang, Z. Wu, Z. Ning, X. & Tiwari, P. (2024). A blockchain-enabled privacy-preserving authentication management protocol for Internet of Medical Things, *Expert Systems with Applications*, vol. 237, pp.121329.
- [13] Haque, E. U. Shah, A. Iqbal, J. Ullah, S. S. Alroobaea, R. & Hussain, S. (2024). A scalable blockchain based framework for efficient IoT data management using lightweight consensus, *Scientific Reports*, vol.14, no.1, pp. 7841.
- [14] Bakhtiary, V. Mirabi, M. Salajegheh, A. & Erfani, S. H. (2024). Combo-Chain: Towards a hierarchical attribute-based access control system for IoT with smart contract and sharding technique, *Internet of Things*, vol. 25, pp. 101080.
- [15] Kiran, A. Mathivanan, P. Mahdal, M. Sairam, K. Chauhan, D. & Talasila, V. (2023). Enhancing data security in IoT networks with blockchain-based management and adaptive clustering techniques, *Mathematics*, vol.11, vol. 9, pp. 2073.
- [16] Huang, R. Yang, X. & Ajay, P. (2023). Consensus mechanism for software-defined blockchain in internet of things, *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 52-60.
- [17] Alshudukhi, K. S. Khemakhem, M. A. Eassa, F. E. & Jambi, K. M. (2023). An interoperable blockchain security frameworks based on microservices and smart contract in IoT environment, *Electronics*, vol. 12, no. 3, pp. 776.
- [18] Zhao, Y. Li, Q. Yi, W. & Xiong, H. (2023). Agricultural IoT data storage optimization and information security method based on blockchain, *Agriculture*, vol.13, no. 2, pp. 274.
- [19] Solomon, G. Zhang, P. Brooks, R. & Liu, Y. (2023). A secure and cost-efficient blockchain facilitated IoT software update framework, *IEEE Access*, vol. 11, pp. 44879-44894.
- [20] Abdi, A. I. Eassa, F. E. Jambi, K. Almarhabi, K. Khemakhem, M. Basuhail, A. & Yamin, M. (2022). Hierarchical blockchain-based multi-chaincode access control for securing IoT systems, *Electronics*, vol. 11, no. 5, 711.
- [21] Qi, L. Tian, J. Chai, M. & Cai, H. (2023). LightPoW: A trust based time-constrained PoW for blockchain in internet of things, *Computer Networks*, vol. 220, pp.109480.
- [22] Ciotta, V. Mariniello, G. Asprone, D. Botta, A. & Manfredi, G. (2021). Integration of blockchains and smart contracts into construction information flows: Proof-of-concept, *Automation in Construction*, vol. 132, pp. 103925.
- [23] Morar, C. D. & Popescu, D. E. (2024). A Survey of Blockchain Applicability, Challenges, and Key Threats, *Computers*, vol. 13, no. 9, pp. 223.
- [24] Stanco, G. Navarro, A. Frattini, F. Ventre, G. & Botta, A. (2024). A comprehensive survey on the security of low power wide area networks for the Internet of Things, *ICT Express*.
- [25] Maghrabi, L. A. (2024). Automated network intrusion detection for internet of things security enhancements. *IEEE Access*.

- [26] Serrano, W. (2024). CyberAI Bot: Artificial Intelligence in an Intrusion Detection System for CyberSecurity in the IoT, *Future Generation Computer Systems*, pp. 107543.
- [27] Pramilarani, K. & Kumari, P. V. (2024). Cost based random forest classifier for intrusion detection system in internet of things, *Applied Soft Computing*, vol. 151, pp. 111125.
- [28] Alzahrani, R. J. & Alzahrani, A. (2023). A novel multi algorithm approach to identify network anomalies in the IoT using Fog computing and a model to distinguish between IoT and Non-IoT devices, *Journal of Sensor and Actuator Networks*, vol. 12, no. 2, pp.19.
- [29] Catillo, M. Pecchia, A. & Villano, U. (2023). A deep learning method for lightweight and cross-device IoT botnet detection, *Applied Sciences*, vol. 13, no. 2, pp. 837.
- [30] Liu, X. Du, Y. (2023). Towards Effective Feature Selection for IoT Botnet Attack Detection Using a Genetic Algorithm. *Electronics*, vol. 12, pp. 1260, <https://doi.org/10.3390/electronics12051260>
- [31] de Caldas Filho, F. L., Soares, S. C. M., Oroski, E., de Oliveira Albuquerque, R., Da Mata, R. Z. A., De Mendonça, F. L. L., & de Sousa Júnior, R. T. (2023). Botnet detection and mitigation model for IoT networks using federated learning, *Sensors*, vol. 23, no. 14, pp. 6305.
- [32] Halgamuge, M. N. & Niyato, D. (2025). Adaptive edge security framework for dynamic IoT security policies in diverse environments, *Computers & Security*, vol. 148, pp.104128.
- [33] Babu, E. S. SrinivasaRao, B. K. N. Nayak, S. R. Verma, A. Alqahtani, F. Tolba, A., & Mukherjee, A. (2022). Blockchain-based Intrusion Detection System of IoT urban data with device authentication against DDoS attacks, *Computers and Electrical Engineering*, vol. 103, pp. 108287.
- [34] Salb, M. Jovanovic, L. Bacanin, N. Antonijevic, M. Zivkovic, M. Budimirovic, N. & Abualigah, L. (2023). Enhancing internet of things network security using hybrid cnn and xgboost model tuned via modified reptile search algorithm, *Applied Sciences*, vol. 13, no. 23, pp.12687.
- [35] Ciric, V. Milosevic, M. Sokolovic, D. & Milentijevic, I. (2024). Modular deep learning-based network intrusion detection architecture for real-world cyber-attack simulation, *Simulation Modelling Practice and Theory*, vol. 133, pp. 102916.
- [36] Alotaibi, B. (2023). A survey on industrial Internet of Things security: Requirements, attacks, AI-based solutions, and edge computing opportunities, *Sensors*, vol. 23, no. 17, pp. 7470.
- [37] Ramos-Cruz, B. Andreu-Perez, J. & Martínez, L. (2024). The cybersecurity mesh: A comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research, *Neurocomputing*, pp. 127427.
- [38] Perazzo, P. Righetti, F. La Manna, M. & Vallati, C. (2021). Performance evaluation of attribute-based encryption on constrained IoT devices, *Computer Communications*, vol. 170, pp. 151-163.
- [39] Muneeswari, G. Varun, S. S. Hegde, R. Priya, S. S. Shermila, P. J. & Prasanth, A. (2023). Self-diagnosis platform via IOT-based privacy preserving medical data, *Measurement: Sensors*, vol. 25, pp. 100636.
- [40] Ismail, E. G. Chahboun, A. & Raissouni, N. (2020). Fernet Symmetric Encryption Method to Gather MQTT E2E Secure Communications for IoT Devices.
- [41] Li, B. Feng, Y. Xiong, Z. Yang, W. & Liu, G. (2021). Research on AI security enhanced encryption algorithm of autonomous IoT systems, *Information sciences*, vol. 575, pp. 379-398.
- [42] Panagiotou, P. Sklavos, N. Darra, E. & Zaharakis, I. D. (2020). Cryptographic system for data applications, in the context of internet of things, *Microprocessors and Microsystems*, vol. 72, pp. 102921.
- [43] Riad, K. & Cheng, J. (2021). Adaptive XACML access policies for heterogeneous distributed IoT environments, *Information Sciences*, vol. 548, pp. 135-152.
- [44] Li, B. Feng, Y. Xiong, Z. Yang, W. & Liu, G. (2021). Research on AI security enhanced encryption algorithm of autonomous IoT systems, *Information sciences*, vol. 575, pp. 379-398.
- [45] Alzubi, J. A. (2021). Blockchain-based Lamport Merkle digital signature: authentication tool in IoT healthcare, *Computer Communications*, vol. 170, pp. 200-208, <https://doi.org/10.1016/j.comcom.2021.02.002>.
- [46] Sheikhpour, S. Ko, S. B. & Mahani, A. (2021). A low cost fault-attack resilient AES for IoT applications. *Microelectronics Reliability*, vol. 123, pp. 114202.
- [47] Salim, M. M. Kim, I. Doniyor, U. Lee, C. & Park, J. H. (2021). Homomorphic encryption based privacy-preservation for iomt, *Applied Sciences*, vol. 11, no. 18, pp. 8757.
- [48] Musthafa, A. S. Preya, A. J. Alneyadi, F. M., Alattas, N. S. El Hassan, G. & Zia, H. (2023, November). Safeguarding IoT Device Deployment in Healthcare: Analysis and Strategies for Enhanced Security and Privacy, In 2023 4th International Conference on Communications, Information, Electronic and Energy Systems (CIEES) (pp. 1-7). IEEE, <https://doi.org/10.1109/CIEES58940.2023.10378838>.
- [49] Ali, A. Pasha, M. F. Ali, J. Fang, O. H. Masud, M. Jurecut, A. D. & Alzain, M. A. (2022). Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: A novel approach to cryptography, *Sensors*, vol. 22, no. 2, pp. 528, <https://doi.org/10.3390/s22020528>.
- [50] Patil, K. S. Mandal, I. & Rangaswamy, C. (2022). Hybrid and Adaptive Cryptographic-based secure authentication approach in IoT based applications using hybrid encryption, *Pervasive and Mobile Computing*, vol. 82, pp. 101552, <https://doi.org/10.1016/j.pmcj.2022.101552>.
- [51] Parmar, M. & Shah, P. (2023). Internet of things-blockchain integration: a robust data security approach for end-to-end communication. *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 32, no. 2, pp. 1050-1057.
- [52] Anitha, S. Saravanan, S. & Chandrasekar, A. (2023). Trust management based multidimensional secure cluster with RSA cryptography algorithm in WSN for secure data transmission. *Measurement: Sensors*, vol. 29, pp.100889.
- [53] El-Hadedy, M. Guo, X. Yoshii, K. Cai, Y., Herndon, R., Banta, B. & Hwu, W. M. (2023). RECO-ASCON: Reconfigurable ASCON hash functions for IoT applications, *Integration*, vol. 93, pp. 102061.
- [54] Abikoye, O. C., Oladipupo, E. T., Imoize, A. L., Awotunde, J. B., Lee, C. C., & Li, C. T. (2023). Securing critical user information over the internet of medical things platforms using a hybrid cryptography scheme, *Future Internet*, vol. 15, no. 3, pp. 99.
- [55] Mohammed, Z. K. Mohammed, M. A. Abdulkareem, K. H. Zebari, D. A. Lakhani, A. Marhoon, H. A. ... & Martinek, R. (2024). A metaverse framework for IoT-based remote patient monitoring and virtual consultations using AES-256 encryption, *Applied Soft Computing*, vol. 158, pp. 111588, <https://doi.org/10.1016/j.asoc.2024.111588>.
- [56] Puthiyidam, J. J., Joseph, S., & Bhushan, B. (2024). Temporal ECDSA: A timestamp and signature mask enabled ECDSA algorithm for iot client node authentication. *Computer Communications*, vol. 216, pp. 307-323, <https://doi.org/10.1016/j.comcom.2024.01.016>.
- [57] Adeniyi, A. E. Jimoh, R. G. & Awotunde, J. B. (2024). A systematic review on elliptic curve cryptography algorithm for internet of things: Categorization, application areas, and security, *Computers and Electrical Engineering*, vol. 118, pp. 109330.
- [58] Hu, Z. Li, J. & Wilson, C. (2024). Resilient intermediary-based key exchange protocol for IoT. *ACM Transactions on Internet of Things*, vol. 5, no. 1, pp. 1-31.
- [59] Silicon Labs. AN1233: Zigbee Security, Rev. 0.4, Copyright © 2023 by Silicon Laboratories. Available online:

<https://docs.silabs.com/zigbee/7.4.2/zigbee-security-overview/>
(accessed on 27.02.2025)

[60] Eyad, M.H.; Samer, A.; Amer, A.; Omar, A.S. Implementing and developing multi-stage cryptography technique for low-cost long-range communication system. *Bull. Electr. Eng. Inform.* 2024, 13.1, 264–276. <https://doi.org/10.11591/eei.v13i1.6989>.

[61] Hamad, E. M. Alabed, S. Alsaraira, A. & Saraereh, O. A. (2024). Implementing and developing multi-stage cryptography technique for low-cost long-range communication system, *Bulletin of Electrical Engineering and Informatics*, vol. 13, no. 1, pp. 264-276.