Journal of Artificial Intelligence and Computing (JAIC)
ISSN (e): 3005-3358
Volume: 4, Number: 1, Pages: 1 - 7, Year: 2026

Cybersecurity Challenges, Vulnerabilities, and Emerging Security Solutions in the Internet of Things

Eeman Khokhar and Irshad Ahmed

Department of Computer Science, University of Management and Technology, Lahore, Pakistan
Corresponding author: Eeman Khokhar (Email: eemansalman4@gmail.com)

Received: 12/02/2026, Revised: 16/05/2026, Accepted: 10/06/2026

***Abstract*— IoT has been revolutionising the world of digital ecosystems by enabling smart, interconnected devices to exchange information across domains such as healthcare, transportation, industry, smart cities, and many others. As IoT expands, emerging cybersecurity challenges stem from resource constraints, heterogeneity, weak authentication, software vulnerabilities, and insecure channels. The proposed survey discusses the prominent security challenges and vulnerabilities in IoT frameworks and presents potential solutions like lightweight cryptography, blockchain, AI-powered IDS, federated learning, and secure authentication schemes. The research highlights the importance of a layered and flexible security approach to enhance IoT security posture, covering its confidentiality, integrity, and availability, so that we can build a secure and robust IoT world.**

Keywords: **Internet of Things (IOT), Cybersecurity, Vulnerabilities, Artificial Intelligence, Authentication, Blockchain.**

I. INTRODUCTION

One of the fastest-growing trends in the current era of information technology is the Internet of Things (IoT), which enables physical devices—ranging from household appliances to heavy machinery—to communicate and exchange data with other devices and become intelligent over the Internet [1-3]. From healthcare and transportation to industrial automation, farm fields, and smart homes and cities, these are the areas where IoT is growing rapidly. IoT helped increase productivity, efficiency, and experience by enabling real-time monitoring, automation, and data analysis to support informed decision-making [4-6].

However, IoT devices have always had vulnerabilities and are prone to cybersecurity attacks. IoT devices can be as small and simple as sensor devices or as complex as the machines used for industrial control. Typically, IoT devices have limited memory, processing power, storage, and energy. These constraints make it challenging to implement security measures that we take for granted on larger systems, such as robust encryption and state-of-the-art intrusion detection systems. As a result, these weaknesses are frequently exploited by cybercriminals [7-10]. Another challenge is the numerous variations of IoT implementations across hardware platforms, operating systems, communication protocols, and even manufacturers. This diversity makes it difficult to create and implement secure and scalable security solutions [11-16].

IoT devices with extended operating lifespans pose a distinct security challenge alongside resource limitations and heterogeneity. Many IoT devices go for years without firmware upgrades or maintenance, in contrast to traditional IT equipment, which is updated and replaced regularly. This would mean that, in the event of a vulnerability being identified, it could take years to be corrected, leaving devices vulnerable and exploitable at all times [15, 17-21]. Another commonly overlooked aspect is physical security. In fact, many IoT devices are installed in areas where they can easily be accessed or misused and where malicious hardware could be easily inserted that can seriously circumvent the network-level defenses [16, 22-27].

Numerous real-world applications have already shown the effects of IoT security flaws. In the healthcare sector, linked medical equipment such as patient monitoring systems, insulin pumps, and wearable health trackers continuously collect and send sensitive patient information. Although these technologies raise the standard of healthcare services, they are appealing targets for fraudsters. A successful cyberattack on these devices has the potential to compromise patient safety and treatment results in addition to exposing private medical records and interfering with vital healthcare procedures. These instances demonstrate the importance of implementing robust yet lightweight security measures that perform well in resource-constrained IoT contexts [28-31].

In a similar vein, IoT-enabled sensors and communication networks are becoming increasingly necessary for smart city infrastructure to control public transportation, traffic flow, energy use, and environmental monitoring. For instance, real-time data from linked sensors is used by intelligent traffic management systems to reduce congestion and enhance road safety. Attackers could, however, alter traffic lights, interfere with transportation services, or produce erroneous data that influences decision-making procedures if they are able to

access these systems without authorization. These situations show that IoT security is now crucial for ensuring the reliability, security, and continuity of vital public services, rather than merely safeguarding digital data.

Real-time monitoring, threat detection, authentication, action, and incident response are more challenging due to the decentralized architecture of IoT networks [5]. Vulnerabilities like weak or default authentication, unencrypted and unsecured communication, outdated firmware, inadequate physical controls, and mishandled sensitive personal data have multiplied as more interconnected devices generate and communicate data at all times. Data breaches, service disruptions, financial losses, and invasions of human privacy and physical safety in critical systems such as industrial control systems and healthcare facilities are examples of security vulnerabilities that can make the environment unsafe [14].

Meanwhile, it's the same story with the growing cybersecurity issues in IoT solutions, which have paved the way for new offerings. However, due to resource constraints on IoT devices, it is crucial to develop lightweight cryptographic algorithms that provide strong protection [6]. As machine learning and artificial intelligence technologies are widely used, autonomous, real-time anomaly detection and automatic responses to new threats are possible [7]. Energy-efficient security mechanisms focus on robust security and operation in small energy resources of the IoT devices [9], and blockchain technology provides decentralized trust infrastructures with improved data integrity and identification without the need for a central point of trust [8]. A goal of standardization activities and interoperability is to create security frameworks that are flexible to various hardware and software IoT systems [10]. Further, the use of emerging technologies such as blockchain and artificial intelligence (AI) in IoT security systems and edge computing approaches for filtering threats in real time in widely deployable networks is among the possible solutions for building secure IoT ecosystems [11] [13].

The purpose of this research paper is to provide an in-depth look to the cybersecurity threats, vulnerabilities, and technologies within IoT environments, as well as the security solutions that will be needed (see Fig. 1). The paper addresses the main security risks to both IoT hardware and networks. Additionally, it reviews recent advances in research and describes advanced approaches to enhance the security, privacy, and resilience of future IoT ecosystems. Those include: lightweight cryptographic techniques; machine-learning-based intrusion detection systems (IDS); blockchain- based trusted models; secure authentication mechanisms; network segmentation; and security-by-design. This table shows the main security risks of IoT systems, where they originate, and how they can be mitigated. These vulnerabilities result primarily from factors such as inadequate security measures, inconsistencies, and limited device capabilities (e.g., insufficient memory). Due to many other challenges (such as outdated firmware) and default configurations,) IoT devices are highly vulnerable to attacks. Therefore, these factors significantly increase the risk of attack, making it difficult to provide adequate protection for IoT systems (see Tab. I).

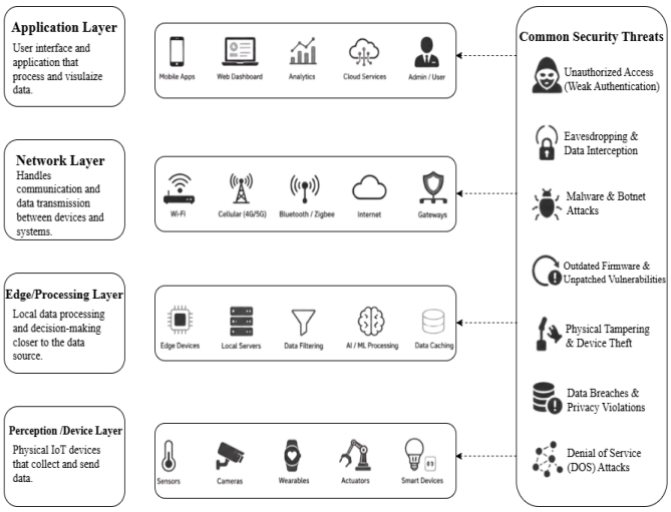

Fig. 1: IOT Architecture and associated Security Threats

Table I: Comprehensive IoT Security Challenges and Root Factor

Security Challenge	Underlying Factors	Impact on IoT Systems	Severity
Resource constraints	Limited CPU, memory, and battery capacity	Restricts strong encryption and IDS deployment	High
Device heterogeneity	Diverse hardware, OS, and protocols	Lack of unified security standards	High
Lack of firmware updates	Infrequent or no patch management	Persistent exploitable vulnerabilities	Critical
Weak default configurations	Factory-set credentials, open ports	Easy unauthorized access	Critical
Physical exposure	Unsecured deployment environments	Device tampering or hardware injection	High

The rest of this document is structured as follows: IoT security issues pertaining to device limitations, heterogeneity, and unsafe communication contexts are covered in Section II. Key IoT vulnerabilities, including obsolete firmware, inadequate encryption, weak authentication, and physical security threats, are highlighted in Section III. Lightweight cryptography, blockchain, AI-based intrusion detection, and federated learning are just a few of the security options that are reviewed in Section IV. A comparison of various methods is given in Section V, together with an outline of their advantages and disadvantages. The study concludes in Section VI, which also offers recommendations for future lines of inquiry into safe IoT systems.

II. An Overview of IoT security issues, Weaknesses, and recent research

IoT devices can range from simple, such as sensors, to complex, such as those used in industrial control applications. They come in various forms, such as hardware architectures, operating systems, and communications

protocols. For this reason, it is very hard to create universally applicable security standards for this problem; if a solution is devised for a high-power smart device, it may not work for a low-power sensor. This is closely related to the problem of resource limitations. With the focus on cost reduction and longer battery life, many IoT devices, especially mobile and environmental sensors, are inexpensive and have minimal computing, memory, and storage requirements. Traditional security protocols such as robust encryption and multi-factor authentication can be daunting and challenging, even leading to trade-offs between security and performance. The main reason why there is such a large number of "inadequate" or default passwords (and lack of encryption and secure boot) assigned to IoT devices is primarily due to manufacturing time and cost over good security, and the growing attack surface created by the large number of interconnected devices is also a major challenge with IoT systems. Each connected device represents a potential entry point for attackers, and even a small vulnerability in a single device may affect the entire system. To illustrate this concept, if a single thermostat or smart light bulb in a smart home is compromised, the attacker may gain access to more critical devices, such as security cameras or smart locks. Thus, securing IoT requires protecting the entire ecosystem as an interlinked network in addition to securing individual devices.

Lastly, IoT devices typically utilize the same device for an extended period of time. Traditional IT equipment is continuously upgraded and replaced with newer software and firmware versions. On the other hand, most IoT devices will operate for years without requiring firmware updates. Therefore, when vulnerabilities are identified in IoT devices, they are often left unpatched/unaddressed for a long time; and

Finally, IoT systems have a high degree of complexity due to the number of devices communicating across local, cloud, and/or industrial environments. As each node can serve as an entry point into the network, the need for a multi-level security approach (hardware, software, monitoring, and rapid response) is clear [3].

Thus, there is an ever-increasing demand for IoT-specific security approaches that are both lightweight and effective in addressing the challenges described above. To address these challenges without imposing an unreasonable burden on resource-constrained devices, researchers are investigating new methodologies, including edge computing-based security, lightweight cryptography, and AI-based anomaly detection.

These techniques aim to maintain the effectiveness and scalability of IoT systems while balancing security and performance. The quick development of IoT technology will continue to pose significant security threats in both personal and commercial applications in the absence of such specialist solutions (see Fig. 2).

III. Analysis of Common IoT Vulnerabilities

Building on these fundamental issues, several specific vulnerabilities in IoT ecosystems have been found to be highly significant. Weak authentication and authorization systems make it easy for hackers to get illegal access and control due to the use of default credentials and because multi-factor authentication is not yet available [5].

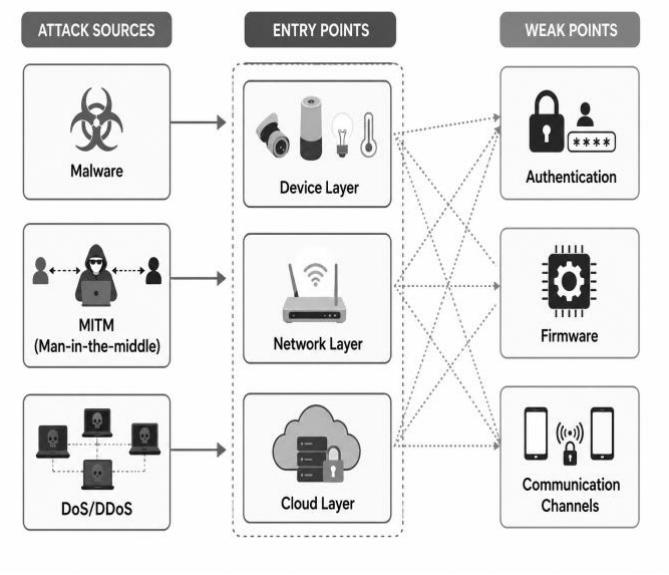

Fig. 2: IoT Threat Model / Attack Surface Diagram

The expansion of the IoT has significantly increased the overall attack surface due to the large number of interconnected devices. In such environments, every device within an IoT network can potentially act as an entry point for malicious actors. As a result, even a minor vulnerability in a single device may compromise the security of the entire system. IoT attacks occur because many connected systems are unsecured and poorly monitored. Additionally, since IoT devices operate at the edge of a network, they typically lack robust cybersecurity tools such as firewalls and intrusion detection/prevention systems (IDPS). There are numerous methods attackers use to get to other parts of an organization's system after getting into one IoT device. One method used is called lateral movement. Lateral movement occurs when hackers move laterally within a target organization's internal network to steal sensitive information or disrupt operations. Hackers accomplish this by finding ways to connect to additional IoT devices on the same internal network. The hacker then uses these new connections to obtain access to more valuable resources, such as business applications, databases, and critical infrastructure.

Another way hackers attack multiple devices is by using something called a botnet. A botnet is a collection of compromised computers or mobile devices that communicate remotely with each other via the internet. When hackers control these devices together in a botnet, they can create powerful distributed denial-of-service (DDoS) attacks against websites, networks, or organizations. Botnets can also be used to commit other types of cybercrime, such as spreading malware. They may even send spam messages.

Attackers may breach a smart home device, such as a light bulb or thermostat, to use it as a bridge to reach other, more secure items. If the attacker gets access to those more secure items – for example, smart door lock or surveillance camera — it would allow them to potentially take over the entire smart home. This illustrates that IoT security is more than just securing individual devices; it also involves maintaining the reliability and trustworthiness of all connected elements within the larger IoT environment.

Data transmitted between IoT devices and cloud servers is often not properly encrypted, leaving it vulnerable to misuse and interception. Examples include the exposure of vital health data from wearable devices or critical data from smart home systems. Devices that fail to receive periodic firmware updates are also vulnerable to previously identified security weaknesses that attackers can easily exploit. Publicly located or unprotected devices pose another threat of exploitation by attackers who can physically modify or reprogram them. Since IoT devices gather large volumes of private and behavioural data, poor management of this data poses high risks of identity theft, violations of consumer privacy rights, and compliance violations, such as those under the EU General Data Protection Regulation (GDPR) [14].

Table II: Detailed IoT Vulnerabilities and Security Implications

Vulnerability Type	Technical Weakness	Security Risk	Possible Attack Outcome
Weak authentication	Default/low-strength credentials	Unauthorized system access	Device takeover
Lack of encryption	Plaintext data transmission	Data interception (MITM attacks)	Privacy leakage
Outdated firmware	No timely patch deployment	Exploitation of known CVEs	Persistent backdoor access
Physical insecurity	Unprotected deployment sites	Hardware tampering	Malicious firmware injection
Poor data governance	Improper handling of sensitive data	Regulatory violations	Identity theft & compliance failure

Table II lists many IoT vulnerabilities, their technical flaws, and potential security threats. It demonstrates how problems such as inadequate encryption and insufficient authentication can quickly lead to unauthorised access and data interception. The likelihood of system compromise and malicious alterations is further increased by outdated firmware and physical vulnerabilities. In general, inadequate data management procedures can also lead to major problems with compliance and privacy.

IV. Evaluation of Current Studies and Suggested Remedies

In IoT networks, securely distributing group keys to low-computational-power services is a challenge. To mitigate this, a software-defined networking (SDN)-based centralized management framework was developed, which involved an improved version of the one-way function tree (MOFT) protocol with collusion attack resistance secured by a formal security analysis and also reduced communication overhead by 39% compared to the traditional OFT protocols [15].

To ensure the safety of vehicle-to-infrastructure (V2I) communication, a new authentication method for Internet of Vehicles (IoV) was proposed based on fuzzy extractors, Elliptic Curve Cryptography (ECC), and Physical Unclonable Functions (PUFs). This way, one can use public-key cryptography without the need for expensive bilinear pairings. The protocol is less computationally or communication-intensive than similar protocols, offers full forward secrecy with Diffie-Hellman values, and is immune to roadside unit side-channel and capturing attacks [16].

Weak authentication based on Physical Unclonable Functions (PUFs) and chaotic maps was proposed to defend the sensors and gateways of underwater acoustic networks (UANs) considering the critical energy constraints and capture concerns of the underwater networks. This protocol has been shown to be useful for security in various hostile IoT environments with resource constraints and has been formally proved in the random oracle model [17].

A Collaborative Intrusion Detection System (CIDS) based on an edge-fog-cloud architecture and Federated Learning (FL) was proposed to address intrusion detection challenges. The solution was found to be superior in terms of network traffic and training time compared with traditional centralised intrusion detection models, using a non-IID subset of the CICIoT2023 dataset [18], with low latency and low resource consumption while maintaining detection accuracy.

An automated approach called VARIoT was developed to generate a comprehensive vulnerability database due to the need for better vulnerability information. Using machine learning, natural language processing, and specialised filters, VARIoT automatically extracts vulnerability descriptions, links them to the corresponding exploit codes from unstructured sources, and assigns a confidence score to each vulnerability to highlight critical vulnerabilities even when information about the product is limited.

A comprehensive security analysis was performed on the Web of Things (WoT), including the creation of threat models for denial-of-service, man-in-the-middle, injection, and physical attacks. The study presented an architecture that provides the necessary level of protection for safe WoT deployments by including isolation features, data encryption, and authentication, as shown in sequence diagrams and UML [20].

In addition to technology solutions for IoT security, there have been studies on the psychology of how individuals react emotionally to cyber-attacks targeting their smart home devices. The study demonstrated that consumers experience the highest degree of emotional response to cyber-attacks on their smart cameras, and that awareness of the occurrence of a breach results in a significant increase in the size of consumer emotional responses to the attack from a combination of questionnaires, an online survey, and a field test [21].

V. Comparative analysis of modern IoT SECURITY SOLUTIONS

The strengths and weaknesses of various contemporary methods for protecting the security of IoT (Internet of Things) devices, using different technologies and operational procedures, are demonstrated in this table. AI-based IDS can intelligently detect threats; however, lightweight cryptography is suitable for low-power devices. Use of blockchain technology will increase both data integrity and user confidence in state data; however, u it may create processing delays and

increase the cost of storing processed data. As such, each method has its own advantages and disadvantages, and no single method can provide adequate protection for all IoT ecosystems (Tab. III).

Table III: Comparative Analysis of IoT Security Solutions

Security Solution	Core Technology	Working Mechanism	Advantages	Limitations
Lightweight Cryptography	Symmetric/asymmetric optimized algorithms	Reduces computational overhead for IoT devices	Energy-efficient, fast processing	Lower security strength vs heavy crypt
AI/ML-based IDS	Machine learning & anomaly detection	Detects abnormal behavior in real-time	Adaptive & intelligent threat detection	Requires training data & computation
Blockchain Security	Distributed ledger technology	Decentralized trust & immutable records	High integrity & transparency	High latency & storage cost
Federated Learning IDS	Edge + cloud collaborative learning	Trains models without sharing raw data	Privacy-preserving, scalable	Complex implementation
PUF-based Authentication	Hardware-based unique identity	Uses physical device fingerprints	Strong device authentication	Hardware dependency

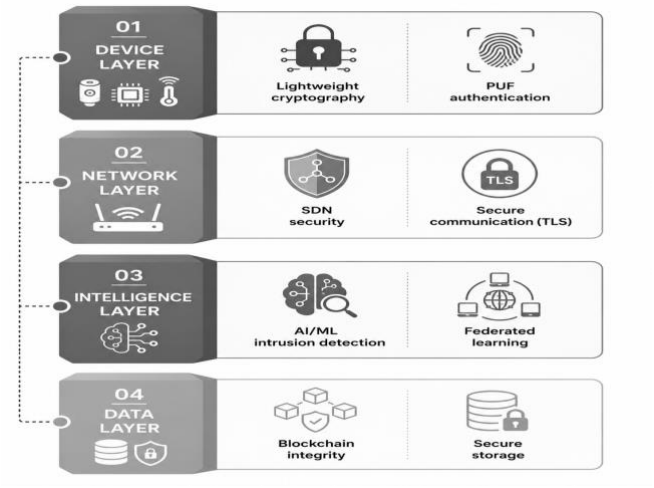

Fig. 3: IoT Security Solution Framework.

The table below shows a multi-layer security design for IoT systems, with each layer performing unique security responsibilities. The Network Layer provides secure communication between devices (Fig. 3). The Device Layer focuses on authenticating and encrypting devices themselves. Data Layer protects the confidentiality and integrity of all data that are being stored. The Processing Layer uses sophisticated methods to detect threats. In summary, the use of layers allows for a structured and effective approach to securing IoT Environments (Tab. IV).

Table IV: Layered IoT Security Architecture Mapping

Layer	**Security Function**	**Example Technologies**	**Purpose in IoT Security**
Device Layer	Authentication & Encryption	PUF, Lightweight Cryptography	protects hardware-level data and verifies identification to secure individual IoT devices.
Network Layer	Secure Communication	TLS, SDN-based Control	guarantees secure data transfer between linked devices and guards against interception.
Processing Layer	Threat Detection	AI/ML-based Intrusion Detection	Real-time detection of cyber risks and aberrant behavior.
Data Layer	Integrity & Privacy Protection	Blockchain, Cryptographic Hashing	preserves tamper resistance, confidentiality, and data integrity.

Table V: IoT Security Overview

Category	Key Points	Security Impact / Role
Security Challenges	Resource constraints, device heterogeneity, lack of firmware updates, weak default configurations, physical exposure	Reduce ability to apply strong security, create large attack surface, increase system vulnerability
Vulnerabilities	Weak authentication, lack of encryption, outdated firmware, physical insecurity, poor data handling	Leads to unauthorized access, data interception, device takeover, privacy leakage, and compliance risks
Security Solutions	Lightweight cryptography, AI/ML-based IDS, blockchain security, federated learning, PUF-based authentication	Improve security with low overhead, enable real-time detection, ensure trust, and preserve privacy
Security Architecture Layers	Device, Network, Processing, Data layers with respective security functions	Provides structured protection across all IoT layers ensuring end-to-end security

This table provides a consolidated view of IoT security challenges, vulnerabilities, and corresponding solutions, highlighting the need for a multi-layered and adaptive security approach.

VI. Conclusion

Smart Cities, Transportation, Health Care, Agriculture, etc., have all been enabled by the IoT's Intelligent Communication and Automation capabilities. The emergence of IoT Ecosystems has led to many new security challenges. For example, no standards exist for how Security Measures are implemented; Vast design options create numerous attack surfaces; Long Device Cycles provide hackers with ample time to find vulnerabilities; and limited resources make it difficult for Devices to be properly secured. Despite the rapid development of IoT Systems, they remain vulnerable to Cyber Threats, Data Breaches, and Operational Disruptions due to

several common Vulnerabilities, such as Poor Authentication, Un-Encrypted Communications, Obsolete Firmware, and Physical Insecurity. As the Traditional Security Solutions cannot easily overcome these barriers, newer, lighter-weight methods are beginning to emerge.

Federated Learning, Blockchain-Based Trust Models, Lightweight Cryptography, and AI- Based Intrusion Detection Methods are among the emerging methodologies for enhancing IoT Security. Layered Security Architectures also provide a systematic approach to fully protect Networks, Devices, and Data.

Ultimately, System Security requires a multi-layered, scalable, and adaptive Strategy that balances Device constraints with Security needs. Future research efforts will need to develop an intelligent, standardised, and power-efficient Security Model capable of addressing the continuously evolving nature of the IoT Environment and emerging threats.

FUNDING STATEMENT

The author(s) received no specific funding for this study.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest to report regarding the present study.

AUTHOR CONTRIBUTIONS

Conceptualization, methodology, validation, writing—original draft preparation, writing—review and editing, E.K., I.A.

INSTITUTIONAL REVIEW BOARD STATEMENT

Not applicable.

INFORMED CONSENT STATEMENT

Not applicable.

DATA AVAILABILITY STATEMENT

Data is available on reasonable request.

REFERENCES

[1] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." *Computer networks* 54, no. 15 (2010): 2787-2805.

[2] Weber, Rolf H. "Internet of Things–New security and privacy challenges." *Computer law & security review* 26, no. 1 (2010): 23-30.

[3] Khanam, Shapla, Ismail Bin Ahmedy, Mohd Yamani Idna Idris, Mohamed Hisham Jaward, and Aznul Qalid Bin Md Sabri. "A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things." *IEEE access* 8 (2020): 219709-219743.

[4] Baker, Shatha A., and Ahmed S. Nori. "Internet of things security: a survey." In *International Conference on Advances in Cyber Security*, pp. 95-117. Singapore: Springer Singapore, 2020.

[5] Campos, Enrique Mármol, Pablo Fernández Saura, Aurora González-Vidal, José L. Hernández-Ramos, Jorge Bernal Bernabe, Gianmarco Baldini, and Antonio Skarmeta. "Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges." *Computer Networks* 203 (2022): 108661.

[6] Katagi, Masanobu, and Shiho Moriai. "Lightweight cryptography for the internet of things." *sony corporation* 2008 (2008): 7-10.

[7] Summerville, Douglas H., Kenneth M. Zach, and Yu Chen. "Ultra-lightweight deep packet anomaly detection for Internet of Things devices." In *2015 IEEE 34th international performance computing and communications conference (IPCCC)*, pp. 1-8. IEEE, 2015.

[8] Qian, Yongfeng, Yingying Jiang, Jing Chen, Yu Zhang, Jeungeun Song, Ming Zhou, and Matevž Pustišek. "Towards decentralized IoT security enhancement: A blockchain approach." *Computers & Electrical Engineering* 72 (2018): 266-273.

[9] Hellaoui, Hamed, Mouloud Koudil, and Abdelmadjid Bouabdallah. "Energy-efficient mechanisms in security of the internet of things: A survey." *Computer Networks* 127 (2017): 173-189.

[10] Ishaq, Isam, David Carels, Girum K. Teklemariam, Jeroen Hoebeke, Floris Van den Abeele, Eli De Poorter, Ingrid Moerman, and Piet Demeester. "IETF standardization in the field of the internet of things (IoT): a survey." *Journal of Sensor and Actuator Networks* 2, no. 2 (2013): 235-287.

[11] Bothra, Priyanka, Raja Karmakar, Sanjukta Bhattacharya, and Sayantani De. "How can applications of blockchain and artificial intelligence improve performance of Internet of Things?–A survey." *Computer Networks* 224 (2023): 109634.

[12] Yang, Yuchen, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao. "A survey on security and privacy issues in Internet-of-Things." *IEEE Internet of things Journal* 4, no. 5 (2017): 1250-1258.

[13] Elmassik, Ziad. "Edge Computing in the Internet of Things: A Survey." *Authorea Preprints* (2023).

[14] Obaidat, Muath A., Suhaib Obeidat, Jennifer Holst, Abdullah Al Hayajneh, and Joseph Brown. "A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures." *Computers* 9, no. 2 (2020): 44.

[15] Taurshia, Antony, Jaspher W. Kathrine, J. Andrew, and Jennifer Eunice R. "Securing internet of things applications using software-defined network-aided group key management with a modified one-way function tree." *Applied Sciences* 14, no. 6 (2024): 2405.

[16] Xie, Qi, and Juanjuan Huang. "Improvement of a conditional privacy-preserving and desynchronization-resistant authentication protocol for IoV." *Applied Sciences* 14, no. 6 (2024): 2451.

[17] Xie, Qi, and Ye Yao. "PUF and chaotic map-based authentication protocol for underwater acoustic networks." *Applied Sciences* 14, no. 13 (2024): 5400.

[18] Wardana, Aulia Arif, Grzegorz Kołaczek, and Parman Sukarno. "Lightweight, trust-managing, and privacy-preserving collaborative intrusion detection for internet of things." *Applied Sciences* 14, no. 10 (2024): 4109.

[19] Felkner, Anna, Jan Adamski, Jakub Koman, Marcin Rytel, Marek Janiszewski, Piotr Lewandowski, Rafał Pachnia, and Wojciech Nowakowski. "Vulnerability and attack repository for IoT: addressing challenges and opportunities in Internet of Things vulnerability databases." *Applied Sciences* 14, no. 22 (2024): 10513.

[20] Albarrak, Khalied M. "Securing the Future of Web-Enabled IoT: A Critical Analysis of Web of Things Security." *Applied Sciences* 14, no. 23 (2024): 10867.

[21] Budimir, Sanja, Johnny RJ Fontaine, Nicole MA Huijts, Antal Haans, Wijnand A. IJsselsteijn, Anne-Marie Oostveen, Frederic Stahl et al. "We are not equipped to identify the first signs of cyber–physical attacks: emotional reactions to cybersecurity breaches on domestic internet of things devices." *Applied Sciences* 14, no. 24 (2024): 11855.

[22] Djenna, Amir, Saad Harous, and Djamel Eddine Saidouni. "Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure." *Applied sciences* 11, no. 10 (2021): 4580.

[23] Ge, Mengmeng, Jin B. Hong, Walter Guttmann, and Dong Seong Kim. "A framework for automating security analysis of the internet of things." *Journal of Network and Computer Applications* 83 (2017): 12-27.

[24] Alsaadi, Ebraheim, and Abdallah Tubaishat. "Internet of things: features, challenges, and vulnerabilities." *International Journal of Advanced Computer Science and Information Technology* 4, no. 1 (2015): 1-13.

[25] Miloslavskaya, Natalia, and Alexander Tolstoy. "Internet of Things: information security challenges and solutions." *Cluster Computing* 22, no. 1 (2019): 103-119.

[26] Manukondakrupa, A. C. "Ensemble-enhanced threat intelligence network (EETIN): A unified approach for IoT attack detection." (2024).

[27] Manukondakrupa, A. C. "Fortifying patient Privacy: a Cloud-Based IoT data security architecture in healthcare." *ResearchGate* (2024).

[28] Wang, Kai, Jiaqing Dong, Ying Wang, and Hao Yin. "Securing data with blockchain and AI." *Ieee Access* 7 (2019): 77981-77989.

[29] Scott-Hayward, S. Securing AI-based Security Systems. Geneva Centre for Security Policy, Strategic Security Analysis, (25), 2022.

[30] Schmitt, Marc. "Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection." *Journal of Industrial Information Integration* 36 (2023): 100520.

[31] Venu, S., et al. Secure big data processing in multihoming networks with AI-enabled IoT. Wireless Communications and Mobile Computing 2022.