IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 14, No. 5, October, 2024, pp. 1385-1390
Journal homepage: http://iieta.org/journals/ijsse

# Design and Implementation of Internet of Things (IoT) Framework for Governing Modern Cyber Attacks in Computer Network

Gunturi S. Raghavendra[1*], Ammanabrolu Mounika Yesaswini[2]

[1] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad 500043, India
[2] Department of Electronics and Communication Engineering, Vardhaman College of Engineering, Hyderabad 501218, India

Corresponding Author Email: g.raghavendra@klh.edu.in

https://doi.org/10.18280/ijsse.140505

**Received:** 24 September 2023
**Revised:** 20 December 2023
**Accepted:** 16 January 2024
**Available online:** 31 October 2024

***Keywords:***
*Internet of Things (IOT), cyber, security, attack, framework, risk, machine learning, management*

## ABSTRACT

The Internet of Things (IoT) stands as a robust framework enhancing the effectiveness and convenience of human existence globally. This transformative technology has made significant strides across diverse application fields. However, with the unprecedented proliferation of smart gadgets and their heavy reliance on wireless technologies, the vulnerability to cyber threats has escalated. The escalating threat landscape poses a significant challenge to the seamless operation of IoT devices. In this context, our paper contributes to the existing body of knowledge by uncovering unique findings that shed light on the intricacies of IoT cybersecurity. Our research not only identifies potential vulnerabilities in current IoT security frameworks but also proposes innovative solutions to mitigate emerging risks. Through an in-depth analysis of cyber threats in the IoT ecosystem, we present a nuanced understanding of the evolving landscape. Our study underscores the critical importance of cybersecurity in the IoT domain, positioning it as the second most crucial aspect after data privacy. In particular, we highlight the pressing need for comprehensive measures to address the escalating danger of cyber-attacks. We propose practical strategies for enhancing the security of IoT resources and safeguarding personal information, thereby mitigating cybersecurity risks for both enterprises and consumers. Furthermore, our paper introduces novel methodologies and frameworks for assessing cybersecurity risks within the IoT landscape. These contributions aim to empower governmental and commercial enterprises with effective tools for evaluating and fortifying their IoT security postures. By addressing the gaps in existing cybersecurity approaches, our research strives to advance the field and foster a secure and resilient IoT environment for the benefit of society at large.

## 1. INTRODUCTION

The Internet of Things (IoT) has ushered in a new era, where networks of interconnected devices drive innovation across various industries [1]. However, the widespread and persistent cybersecurity attacks on IoT devices have raised concerns regarding reputations, financial losses, implementation issues, and disruptions in business processes. The rapid proliferation of IoT devices in sectors such as smart metering, environmental monitoring, patient surveillance systems, advanced manufacturing, and transportation has led to a surge in cyber-attacks, exacerbated by the unpredictable and transient nature of device connections, the involvement of multiple organizations in IoT networks, and resource constraints [2].

The global IoT security market is projected to experience substantial annual growth between 2018 and 2023, with an expected annual growth rate of 33.7%. Factors contributing to this growth include the rise in IoT system attacks, the development of IoT security regulations, and heightened security concerns. A recent survey indicates that IoT-based risks are anticipated to become more prevalent and impactful, necessitating increased attention from top-level management to establish organizational-level cyber risk management. Alarmingly, only 35% of survey respondents claim to have an IoT security plan in place, with a mere 28% having implemented it. Another survey reveals that 80% of firms experienced cyber-attacks on their IoT devices in the past year, while 26% failed to deploy security defense technology, underscoring the critical need for proactive investments in IoT protection [3]. IoT cybersecurity aims to mitigate cybersecurity risks for enterprises and consumers by safeguarding IoT resources and privacy. Although new cybersecurity technologies continually emerge, presenting both opportunities and challenges, previous research has predominantly focused on the technical aspects of IoT cybersecurity. Notably, effective risk governance frameworks to address the myriad cybersecurity challenges in IoT systems are lacking [4].

In response to this gap in IoT cybersecurity risk management, this study undertakes a literature analysis on IoT information security and cyber risk governance frameworks. Subsequently, it proposes a four-tier IoT cyber risk organizational framework to provide a comprehensive approach to managing cybersecurity risks in IoT environments. The specific goals and objectives of this study are to identify existing gaps in current IoT cybersecurity practices, analyze the literature for insights into information security and risk governance frameworks, and develop a practical and effective organizational framework for mitigating cyber risks in IoT systems [5].

## 2. CYBER ATTACKS: DEFINITIONS AND ACTORS

A cyber-attack is defined as any effort to obtain unauthorized information from a computer, computing system, or computer network with the goal of causing harm. These attacks seek to damage, interrupt, control computer systems, or manipulate stored information. Cybercriminals, including malicious individuals, hackers, and organized crime groups, conduct these attacks. Government-sponsored gangs of computer professionals, known as nation-state attackers, also engage in cyber assaults, targeting various entities such as governments, corporations, charities, and organizations as shown in Figure 1.

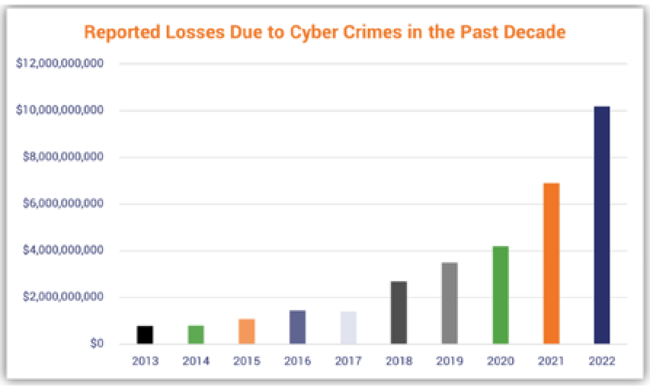

**Figure 1.** Losses reported as a result of a cyber-attack (2013-2022)

### 2.1 Forms of cyber attacks

**Phishing**

*Description:* Attackers manipulate email messages to deceive users into downloading viruses by opening attached documents or clicking on links.

*Real-world example:* The 2016 phishing attack on the Democratic National Committee, leading to unauthorized access and information leaks [6].

**DDoS (Denial-of-Service)**

*Description:* Attackers flood an organization's servers with massive amounts of identical information requests, rendering the server incapable of handling genuine requests.

*Real-world example:* The 2016 Dyn DDoS attack disrupted major internet platforms, affecting users' access to popular websites.

**Zero-day Exploit**

*Description:* Hackers target a newly discovered vulnerability in IT architecture for the first time.

*Real-world example:* The Stuxnet worm utilized multiple zero-day exploits to target Iran's nuclear facilities in 2010.

**Drive-by download**

*Description:* Users unknowingly download viruses when visiting infected websites.

*Real-world example:* The Watering Hole attacks in 2014 targeted specific websites to infect visitors with malware.

**Credential-based attacks**

*Description:* Hackers obtain IT professionals' identities to gain unauthorized access to computers and confidential material.

*Real-world example:* The 2014 Yahoo data breach compromised millions of user accounts through credential theft.

**DNS tunneling**

*Description:* Hackers create a gateway into victims' systems using a compromised Domain Name System (DNS).

*Real-world example:* The Duqu malware utilized DNS tunneling for communication in 2011.

**SQL injection**

*Description:* Hackers inject malicious SQL code into servers to force exposure of confidential material.

*Real-world Example:* The 2017 Equifax breach resulted from an SQL injection, exposing sensitive personal information.

**Man-in-the-middle (MitM):**

*Description:* Attackers position themselves between parties to eavesdrop or manipulate communications.

*Real-world Example:* Wi-Fi eavesdropping during public networks, capturing sensitive information.

**Malware**

*Description:* Harmful software used to target computer systems, including extortion, spyware, and viruses.

*Real-world example:* The WannaCry ransomware attack in 2017 encrypted data, demanding ransom for decryption keys.

## 3. FRAMEWORK FOR IOT

IoT is an expansive network of interconnected devices that has undergone rapid expansion in recent years. This evolution has transformed it into a contemporary-styled network, serving as a crucial facilitator that bridges the physical and digital realms. The applications of IoT are diverse and ever evolving, ranging from its essential role in smartphones to the increasing demand for a variety of gadgets, including cameras, media players, wearable technology, smart TVs, and intelligent virtual reality (VR) systems. However, amidst this technological progress, the landscape of IoT is not without its challenges, particularly the looming threat of cyber-attacks. At its core, the primary functionality of IoT applications lies in the collection of data from digital devices, facilitating interaction through networks [7]. This versatility is evident in various IoT applications, spanning sectors such as sustainable farming, healthcare, home automation, and meetings, accumulating substantial volumes of personalized data [8]. This wealth of information traverses IoT systems, where it undergoes meticulous scrutiny and analysis. Notably, Cisco's study projects an astonishing 50 billion smart gadgets to be connected to the web this year, with these advanced devices expected to seamlessly integrate into daily life in the near future. The anticipation is that the utilization of IoT systems will not only witness a surge but will also undergo sustained expansion. A significant trend has emerged due to the widespread adoption of IoT-acquired data, wherein information gathered from smart devices within an IoT context holds the potential to be transferred and utilized across various real-world applications. However, a considerable impediment in harnessing this information lies in the inherent diversity of smart devices within IoT system design. Effectively managing and extracting meaningful insights from this diverse array of devices poses a formidable challenge for the ongoing development and utilization of IoT technologies.

## 4. CYBERS SECURITY IN INTERNET OF THINGS ARCHITECTURE

Because each level of the Internet of Things design has its own set of security concerns and communicates with the other levels, security solutions should be addressed for the whole system [9]. A survey of the research on cyber security technologies conducted via the lens of the Internet of Things design enables us to get a more systematic and integrated understanding of IoT cyber security. The preceding is focused on the five-layer design of corporate IoT and concentrates on cyber security challenges and solutions at the layers level, rather than at the system level.

### 4.1 The perception layer of cybersecurity

When it comes to the Internet of Things, although many pieces of equipment are meant to be low-power and lightweight, they often capture big quantities of information from the real-world environment and as a result use a variety.

of energy-saving techniques. Technology such as machine learning is often used in order to draw trustworthy conclusions from the information collected [10]. It has been difficult, however, to include integer arithmetic security or confidentiality safeguards into lightweight Internet of Things gadgets, owing to the limited resource capability of these gadgets. At the perception layer, one of the most serious security concerns is the copying of gadget components for the purpose of cyber-attacks. In the case of RFID tags, for instance, copies of the tags might be used to perform widespread denial-of-service assaults (Dodos). Physically unclonable functions (PUFs) have been employed for verification and identifying, as well as for the production of data encryption on a chip, as per [11].

Chips with PUFs improve security by providing tampering resistance, device verification, as well as preventing the use of duplicated equipment. Because the elements of Internet of Things devices are often performed on devices with limited resources, lightweight PUF implementations are necessary [12]. While PUFs themselves cannot be cloned, it is feasible to clone a PUF key after it has been retrieved from a PUF. As a result, a variety of verification techniques based on PUFs have been developed.

### 4.2 Network-level cybersecurity

The networks layers of the Internet of Things systems are critical to the overall protection efficiency of the IoT system, since secure information transfer across the networks is required for the proper operation of gadgets, processing units, and the complete IoT system. An intrusion detection system (IDS) is a system that is used to identify assaults, take remedial action, and analyze data packets [13]. There are several infringement identification techniques used by the IDS: statistical analysis for outlier identification, developmental computation for categorizing interferences error propagation circumstances, behavior and tried intrusions, procedure confirmation for categorizing questionable behaviors, information retrieval techniques such as the spontaneous forest technique, and machine learning for categorizing network infringement trends are just a few of the techniques employed. Machine learning algorithms have shown encouraging results in the identification of distributed denial of service (DDoS) assaults, with the greatest efficiency recorded at 97.16 percent [14]. Hybrid approaches for identifying hostile activity on IoT networks that combine dimensional reductions and categorization algorithms have also shown good results.

### 4.3 Cyber security at the application layer

Professional IoT applications such as management and surveillance, massive data and business intelligence, data exchange and teamwork, and data exchange and teamwork are all frequently employed. Intelligent applications in many domains including home automation, intelligent transportation, intelligent health, and intelligent infrastructures are needed for a variety of security management systems. Smart healthcare, for instance, works with extremely individualized information and hence necessitates the use of increased protection and confidentiality protection. Because many Internet of Things (IoT) apps may be held by third-party service providers, assaults on these apps may have an impact on the security of other interconnected apps [15].

## 5. IOT SECURITY AT ITS FINEST

The integration of AI and ML into IoT security frameworks signifies a groundbreaking approach that holds substantial promise for bolstering the resilience of interconnected systems in the face of the constantly evolving landscape of cyber threats. In the context of IoT security, AI and ML contribute significantly by introducing adaptive and intelligent mechanisms that go beyond traditional rule-based approaches as shown in Figure 2.

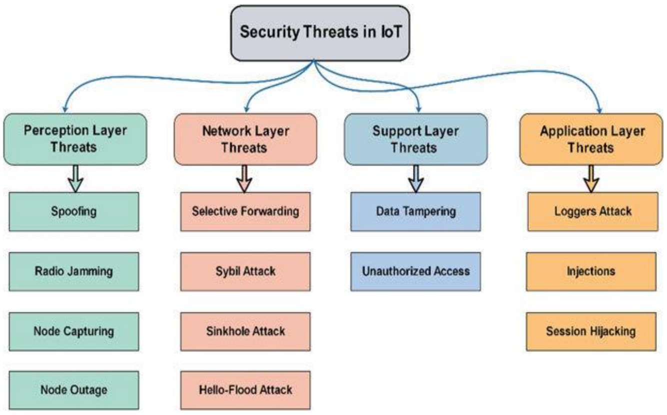

**Figure 2.** Threats and IoT

AI's role in IoT security involves leveraging advanced algorithms to analyze patterns, anomalies, and deviations in real-time data streams from IoT devices. Through the utilization of sophisticated algorithms, AI can rapidly identify and respond to abnormal behaviors that may indicate a potential cyber-attack. This proactive stance is crucial in a landscape where the nature and sophistication of threats are continually mutating [16].

On the other hand, machine learning complements AI by enabling systems to learn and adapt autonomously. ML algorithms can analyze historical data to discern patterns and trends associated with various types of cyber threats. This learning capability empowers the system to evolve and improve its threat detection accuracy over time. Moreover, ML excels in recognizing novel threats that may not fit predefined patterns, thereby providing a more comprehensive and adaptive defense mechanism.

The amalgamation of AI and ML in IoT security frameworks not only enhances the detection capabilities but also facilitates rapid response and mitigation strategies. AI-driven systems can autonomously make decisions based on real-time threat assessments, enabling quick and precise actions to neutralize potential risks. Additionally, the continuous learning aspect of ML ensures that the system remains adept at handling new and emerging threats, contributing to the long-term resilience of IoT ecosystems.

Furthermore, the incorporation of neural networks within AI models enhances the ability to discern complex relationships within vast datasets, aiding in the identification of subtle indicators of cyber threats. Blockchain technology, when integrated into these frameworks, adds an additional layer of security by ensuring the integrity and immutability of data, thereby thwarting unauthorized access and tampering attempts [17].

In conclusion, the symbiotic integration of AI and ML, coupled with advanced technologies like neural networks and blockchain, not only fortifies the defense mechanisms of IoT systems but also positions them to adapt and counteract emerging cyber threats. This holistic approach represents a transformative paradigm in IoT security, fostering a resilient and adaptive response capability crucial for safeguarding the integrity and functionality of interconnected devices in our increasingly connected world [18].

## 6. INTERNET OF THINGS (IOT) CHALLENGES

The integration of blockchain technology into the Internet of Things (IoT) ecosystem addresses various challenges and concerns, providing a robust framework for secure and efficient operation. One notable advantage lies in information manipulation prevention. By intertwining IoT devices using blockchain, the system establishes an immutable ledger, dismissing any attempts to alter or manipulate information through these interconnected gadgets. This ensures the integrity and authenticity of data generated and exchanged within the IoT network. Another significant benefit is observed in price and traffic administration through the decentralization function of blockchain. Rather than relying on centralized servers, IoT gadgets can establish peer-to-peer connections, enhancing efficiency and reducing dependencies on single points of failure. This decentralized approach not only contributes to streamlined communication but also mitigates potential bottlenecks associated with centralized systems [19].

Addressing concerns about confidentiality with IoT gadgets is crucial, and blockchain technology offers a solution through the implementation of permissionless blockchain. This ensures that sensitive data remains secure and private, restricting access only to authorized entities. The transparent and tamper-resistant nature of blockchain contributes to building trust and confidence in the confidentiality of IoT-related information.

Moreover, the issue of lack of proper operation due to severe demand on cloud platforms is mitigated by the blockchain's distributed nature. Information entries are transmitted to various network nodes, eliminating a single weak point. This redundancy ensures that even in the face of high demand, the same information is replicated across nodes, preventing system failures, and ensuring continuous operation.

Architectural flaws in the IoT ecosystem are also addressed through the use of blockchain for validation. The information exchanged within the network is encrypted, providing an additional layer of security to guarantee that it was transmitted by an authorized sender. This helps in preventing unauthorized access, tampering, or malicious activities within the IoT infrastructure.

In summary, the incorporation of blockchain technology into the IoT landscape offers a multifaceted solution, providing security against information manipulation, decentralized communication for improved efficiency, enhanced confidentiality through permissionless blockchain, resilience to high demand on cloud platforms, and validation mechanisms to address architectural flaws. These features collectively contribute to a more secure, efficient, and reliable Internet of Things ecosystem.

## 7. AN ALTERNATIVE TO BLOCKCHAIN TECHNOLOGY IN THEORY

### 7.1 Information distortion and improper use

The data collected from IoT (Internet of Things) devices can be susceptible to distortion and misuse. This can happen due to various reasons, including errors in data collection, transmission, or interpretation. Hackers may also manipulate the data for malicious purposes. For instance, if IoT devices are used for monitoring and controlling critical infrastructure like smart grids or industrial systems, distorted information can lead to incorrect decisions, potentially causing significant damage.

### 7.2 Controlling the rapid expansion of IoT systems

The proliferation of IoT devices has been exponential, and managing the growth of these systems poses a significant challenge. Implementing security measures, updates, and patches across a vast network of devices requires substantial time and resources. This complexity increases the risk of vulnerabilities and security gaps, as it becomes challenging to ensure that every device in the network is properly protected.

### 7.3 Cyber-attacks on user information

As the number of IoT devices increases, so does the attractiveness of these devices as targets for cyber-attacks. Many IoT devices collect and transmit sensitive user information. Cybercriminals may exploit vulnerabilities in these devices to gain unauthorized access, steal personal data, or even launch more extensive attacks on other connected systems. This vulnerability poses a serious threat to user privacy and data security.

### 7.4 Unavailability of cloud services

Many IoT systems rely on cloud services for data storage, processing, and analysis. However, these cloud services are not immune to cyber-attacks, power outages, or software problems. A cyber-attack on a cloud service provider could result in service disruption, making it difficult for IoT devices to function properly. Power outages or software failures in the cloud infrastructure can also lead to unavailability, impacting the performance and reliability of IoT systems [20].

### 7.5 Weaknesses in IoT devices and networks

IoT devices often have inherent vulnerabilities, both in terms of hardware and software. In some cases, manufacturers may prioritize functionality and cost over security during the development process. These weaknesses can be exploited by malicious actors to compromise the integrity and confidentiality of data transmitted by the devices. Additionally, insecure network configurations or lack of proper encryption can expose IoT networks to unauthorized access and manipulation [21].

## 8. REQUIREMENTS

### 8.1 Distorted information from IoT equipment

Information gathered from IoT (Internet of Things) devices may be distorted due to various reasons. This distortion can occur during data transmission, processing, or even when the sensors in the IoT devices are not calibrated or functioning properly.

Improper use may arise when the data collected is misinterpreted, leading to incorrect decisions or actions. For example, if a sensor measuring environmental conditions malfunctions, it might provide inaccurate data that could result in faulty analysis and decision-making [22].

### 8.2 Controlling rapid expansion of IoT systems

The deployment and management of IoT systems involves a large number of devices, each with its own set of configurations, updates, and security considerations.

Controlling the expansion requires meticulous planning and execution to ensure that all devices are integrated seamlessly, adhere to security protocols, and function cohesively. This can be time-consuming and complex, particularly as the number of IoT devices increases.

### 8.3 Cyber attacks on IoT systems

IoT devices are often vulnerable to cyber-attacks, as they may not have robust security measures in place. Cybercriminals can exploit these vulnerabilities to gain unauthorized access to user information stored in IoT devices.

User information being more susceptible means that personal data, such as sensitive health information, location data, or user habits, could be accessed by malicious actors, leading to privacy breaches and potential misuse.

### 8.4 Cloud service unavailability

Many IoT devices rely on cloud services for data storage, processing, and synchronization. However, these cloud services are not immune to cyber-attacks, power outages, or software problems.

A cyber-attack on cloud services can lead to a loss of connectivity and functionality for IoT devices. Additionally, power outages or software issues in the cloud infrastructure can disrupt the services, affecting the operation of connected IoT devices.

### 8.5 Weaknesses in IoT devices and networks

IoT devices often have security weaknesses, such as default passwords, lack of encryption, or outdated firmware. These vulnerabilities can be exploited by attackers to gain unauthorized access or control over the devices.

Weaknesses in the networks connecting IoT devices can also be exploited, leading to unauthorized access, data interception, or disruption of communication between devices.

In summary, these challenges highlight the importance of addressing security concerns, implementing robust management practices, and establishing effective protocols to ensure the proper functioning and secure deployment of IoT systems.

## 9. CONCLUSIONS

The topic outlined appears to focus on various aspects of cybersecurity, with a specific emphasis on cyber-attacks, prevalent forms of cybercrime, the Internet of Things (IoT) architecture, and cybersecurity within the IoT context. Let’s break down each part of the study:

**Introduction to cyber-attack**

The study likely begins with an exploration of the concept of a cyber-attack. This could involve defining what constitutes a cyber-attack, the various methods employed, and the potential consequences.

**Prevalent forms of cybercrime**

Following the introduction, the study may delve into different types of cybercrime. This could include but is not limited to, phishing, malware, ransomware, and other common threats in the digital landscape.

**Framework and application of IoT**

The study then transitions to IoT, providing an overview of the framework and applications. This may involve explaining the basic structure of IoT systems and how they are utilized in various contexts.

**Cybersecurity in IoT architecture**

The focus then shifts to the cybersecurity aspect within the IoT architecture. This section could include discussions on the unique challenges posed by IoT devices, networks, and systems in terms of security.

**Layers of cybersecurity in IoT**

The study may categorize cybersecurity in IoT into different layers for a more structured analysis:

Perception Layer: This might involve security measures at the sensory or data collection level of IoT devices.

Network-Level Cybersecurity: This layer could address security concerns related to the communication and connectivity between IoT devices.

Processing Layer Cybersecurity: Security measures at the data processing level within IoT systems may be explored.

Application Layer Cybersecurity: Finally, the study could discuss security measures implemented at the application or software layer of IoT systems.

**Discussion on IoT security**

The study may conclude with a comprehensive discussion on IoT security, emphasizing best practices, challenges, and potential solutions. This could include the integration of encryption, authentication, and other security protocols.

**IoT security at its finest**

The phrase "IoT security at its finest" likely suggests a deeper exploration into cutting-edge or highly effective security measures within the IoT landscape. This could involve the use of advanced technologies, machine learning, or other innovative approaches to enhance cybersecurity.

In summary, the study seems to provide a holistic examination of cybersecurity, with a particular focus on IoT, covering different layers of security within the architecture and concluding with a discussion on achieving optimal security in the IoT domain.

## REFERENCES

[1] Lee, I. (2019). The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model. Internet of Things, 7: 100078. https://doi.org/10.1016/j.iot.2019.100078

[2] Nurse, J.R., Creese, S., De Roure, D. (2017). Security risk assessment in Internet of Things systems. IT Professional, 19(5): 20-26. https://doi.org/10.1109/MITP.2017.3680959

[3] Banjanin, B., Vladić, G., Adamović, S., Bošnjaković, G. (2022). Global market structure. In Polymers for 3D Printing, pp. 353-367.

[4] Kello, L. (2017). Cyber Security: Gridlock and Innovation. Polity Press.

[5] Kadivar, M. (2014). Cyber-attack attributes. Technology Innovation Management Review, 4(11): 22-27. http://doi.org/10.22215/timreview/846

[6] Tampubolon, K.E.A. (2019). Perbedaan Cyber Attack, Cybercrime, dan Cyber Warfare. Jurist-Diction, 2(2): 539-554.

[7] Andersson, K., You, I., Rahmani, R., Sharma, V. (2019). Secure computation on 4G/5G enabled Internet-of-Things. Wireless Communications and Mobile Computing, 2019: 3978193. https://doi.org/10.1155/2019/3978193

[8] Shin, D., Sharma, V., Kim, J., Kwon, S., You, I. (2017). Secure and efficient protocol for route optimization in PMIPv6-based smart home IoT networks. IEEE Access, 5: 11100-11117. https://doi.org/10.1109/ACCESS.2017.2710379

[9] Xu, H., Ding, J., Li, P., Zhu, F., Wang, R. (2018). A lightweight RFID mutual authentication protocol based on physical unclonable function. Sensors, 18(3): 760. https://doi.org/10.3390/s18030760

[10] Panwar, V., Sharma, D.K., Kumar, K.P., Jain, A., Thakar, C. (2021). Experimental investigations and optimization of surface roughness in turning of en 36 alloy steel using response surface methodology and genetic algorithm. Materials Today: Proceedings, 46: 6474-6481. https://doi.org/10.1016/j.matpr.2021.03.642

[11] Gao, Y., Ranasinghe, D.C., Al-Sarawi, S.F., Kavehei, O., Abbott, D. (2016). Emerging physical unclonable functions with nanotechnology. IEEE Access, 4: 61-80. https://doi.org/10.1109/ACCESS.2015.2503432

[12] Jain, A., Pandey, A.K. (2017). Multiple quality optimizations in electrical discharge drilling of mild steel sheet. Materials Today: Proceedings, 4(8): 7252-7261. https://doi.org/10.1016/j.matpr.2017.07.054

[13] Hodo, E., Bellekens, X., Iorkyase, E., Hamilton, A., Tachtatzis, C., Atkinson, R. (2017). Machine learning approach for detection of nontor traffic. In Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, pp. 1-6. https://doi.org/10.1145/3098954.3106068

[14] Jain, A., Pandey, A.K. (2019). Modeling and optimizing of different quality characteristics in electrical discharge drilling of titanium alloy (Grade-5) sheet. Materials Today: Proceedings, 18: 182-191. https://doi.org/10.1016/j.matpr.2019.06.292

[15] Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B., Bangash, Y.A. (2020). An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security. IEEE Internet of Things Journal, 7(10): 10250-10276. https://doi.org/10.1109/JIOT.2020.2997651

[16] Karie, N.M., Sahri, N.M., Yang, W., Valli, C., Kebande, V.R. (2021). A review of security standards and frameworks for IoT-based smart environments. IEEE Access, 9: 121975-121995. https://doi.org/10.1109/ACCESS.2021.3109886

[17] Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., Ghani, N. (2019). Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. IEEE Communications Surveys & Tutorials, 21(3): 2702-2733. https://doi.org/10.1109/COMST.2019.2910750

[18] Sauter, T., Treytl, A. (2023). IoT-enabled sensors in automation systems and their security challenges. IEEE Sensors Letters, 7(12): 1-4. https://doi.org/10.1109/LSENS.2023.3332404

[19] Adam, M., Hammoudeh, M., Alrawashdeh, R., Alsulaimy, B. (2024). A survey on security, privacy, trust, and architectural challenges in IoT systems. IEEE Access, 12: 57128-57149. https://doi.org/10.1109/ACCESS.2024.3382709

[20] Bouzidi, M., Gupta, N., Cheikh, F.A., Shalaginov, A., Derawi, M. (2022). A novel architectural framework on IoT ecosystem, security aspects and mechanisms: A comprehensive survey. IEEE Access, 10: 101362-101384. https://doi.org/10.1109/ACCESS.2022.3207472

[21] Mutleg, M.L., Mahmood, A.M., Al-Nayar, M.M.J. (2024). A comprehensive review of cyber-attacks targeting IoT systems and their security measures. International Journal of Safety and Security Engineering, 14(4): 1073-1086. https://doi.org/10.18280/ijsse.140406

[22] Dehimi, N.E.H., Tolba, Z., Djabelkhir, N. (2024). Testing inclusive, exclusive, and parallel interactions in multi-agents system: A new model-based approach. International Journal of Safety and Security Engineering, 14(4): 1125-1138. https://doi.org/10.18280/ijsse.140411