Grenze International Journal of Engineering and Technology, January Issue

Analyzing Emerging Cybersecurity Threats in IoT Applications and Service Domains

Piyush Sasmal[1], shalini[2] and Shruti Gupta[3]
[1-3]Manav Rachna International Institute of Research & Studies, Faridabad, India
Email: mr.piyush14344@gmail.com, shalini.kumari0106@gmail.com, Email: shruti.searching@gmail.com

***Abstract*— The research paper talks about the growing security threats in the areas of Internet of Things (IoT) applications and services because of the proliferation of connected devices, disclosing vulnerability to more sophisticated attacks, jeopardizing data integrity, confidentiality, and system reliability. The literature review, methods of threats modelling and case studies that represent various industries, such as healthcare, smart cities, and industrial automation, the analysis decomposes the emergent risks of unauthorized access, malware distribution, and malfunctioning of the supply chains. The key takeaways include the fact that threats tend to have weak authentication protocols and firmware vulnerabilities that lead to the downfall of the grand networked ecosystem. The outstanding conclusion is the need to respond to an integrated approach to security, the importance of possessing active threat intelligence and homogeneous procedures to mitigate the threats and develop resilient IoT structures that eventually improve the security of important services in a more digitized world.**

***Index Terms*— cybersecurity, data integrity, IoT, supply chain, threat modelling.**

I. INTRODUCTION

The Internet of Things (IoT), which is a topic of a contemporary online setting, has proved so attractive and powerful that physical objects are ideally interrelated with the capacity to compute and get more effective, more interconnected, and more mundane in a variety of aspects. Whether it is intelligent homes taking over the daily routine, industry taking over factories in streamlining processes, or IoT applications being implemented everywhere in life, and even in major infrastructure, which adds to the information exchange and the acceleration of the decision-making process [1]. This diffusion is the driving force behind why IoT is a major factor in the economic growth and social advancement, because the web of devices can be accessed to build smarter cities, more technologically advanced health care uses, and more efficient energy utilisation.

The extension of the IoT does indicate its prominent feature in the fourth industrial revolution of billions of sensors, actuators and embedded systems to enable intelligent ecosystems. On a generalisation of trends in terms of the development of the IoT, it is seen that the phenomenon is experiencing a rampant growth, with machines replacing humans not through simple sensors alone but through sophisticated networks that will carry out their own tasks. This growth, in its turn, comes along with the inherent vulnerabilities of its own, and the lack of homogeneity of the IoT architectures, caused by the hardware, the software, and the communication protocols, offers a fertile ground for cybersecurity threats. Previous research has reported on the risks of the start-up stage of the IoT, including the vulnerability of information during the process of exchanging information through weak encryption protocols, the lack of sufficient access control protocols that enable intruders to access the

Grenze ID: 01.GIJET.12.1.115

device, and the discrepancy between the resources or their absence, which limit the implementation of effective security protocols [2].

Denial of service attacks of environments bombarding the networks to devices, tailor-made malware loops taking advantage of the firmware vulnerabilities and loss of privacy as a result of unsecured compilation aggregation environments have been investigated. In one instance, studies on smart grid applications have discovered how the entry of competitors can interfere with the systems of energy delivery through compromised meters, and studies of wearable health devices have discovered threats of possible sensitive medical information breaches. Combined, these pieces of literature focus on the extent to which the nature of insecurities brought by the IoT can be systemic, in many cases due to the lack of standard security practices, and the rate at which the deployment is flung miles ahead of the defensive response operation. Moreover, the automotive IoT research has rendered the perception of these threats to automobile security, such as remote car hijacking via infotainment systems linked to the automobile, obvious, which sheds light on the potential threat of having a combination of both offline oppression and online attacks. Collectively, this literature creates a unity of the multidimensionality of the issues affecting the IoT and therein, cybersecurity is an unavoidable cloak of sustainable implementation [3].

However, despite these advances in awareness of the vulnerabilities of the IoT, a critical analysis has revealed deficiencies in addressing the fluid and emerging nature of threats in specific areas of use and service. Even though past studies have been rather helpful in the field of generic attack vectors, they often omit the context-specific nuances, which make the risks in shifting ecosystems, e.g. the integration of artificial intelligence and the IoT or the switch to edge computing models. Such a retort is suicidally different to traditional frameworks, based on stale threat models, highlighting the adaptive approach applied by contemporary cybercriminals, who apply machine learning in orchestrating sneaky infiltrations or take advantage of zero-day vulnerabilities of supply chain implementation. Moreover, there is also an evident knowledge gap in the literature relating to spectrums of domain-specific needs on top of the topography of threats; whether at the expense of functionality over safety [4], creating gaps in aspects of unresponded exploits that cascade through interrelated services. The effectiveness of the modern mitigation strategies to address complex threats, such as performing targeted threats, such as advanced persistent threats specific to the healthcare IoT, when the integrity of the information of the patients holds utmost importance, or smart city infrastructures vulnerable to coordinated attacks and disruptions to the safety of populations, must be questioned. What are some of the ways emerging threats will adapt to technological convergence, and what are some of the understudied vectors that can bring down the resilience of service-oriented IoT architectures? By posing these questions, this discussion is part of a long-standing academic tradition of analytical development in cybersecurity studies, and elaborates previous studies, pursuing the fine-scale investigation of the perils that optimise relative to the individual constraints and opportunities of different spheres. The given niche shows the need not to cover the discussion of the large-scale propositions but to dwell upon the details determining the emergence and spread of the threat in an age of hyper-connectivity [5].

In order to fill this niche, the current research seeks to thoroughly examine the threats of emerging cybersecurity in search of IoT applications and service sectors, with an enigmatic approach that ties theoretical knowledge with practical considerations. Understanding the purpose of the present study, we will make the situation with the evolving threat scenario clearer, specify the key risk variables and propose how to make the protection more efficient without inventing new frameworks [6]. The research is a systematic review of the current known literature, the threat modelling exercises, along with the detailed case studies based on other areas, including healthcare, smart cities, and industrial automation. This approach eases the dissection of the assault, such as unauthorised access through the utilisation of improper authentication scan, propagation of malware software to nodes, and supply chain lapses that inject evil at the production stage. We apply the qualitative synthesis in the present research to track the domain-specific threat vectors in an exemplification of the differences in the vulnerability to eavesdropping and replay attacks around the world, supported by the low-power nature of IoT affiliates pursuing remote monitoring technologies. The basic findings reveal that new attacks tend to use the gaps in firmware and under-updating of the systems, resulting in massive attacks that propagate throughout the networked ecosystems and disrupt the operations [7]. In e.g. healthcare IoT, these dangers are manifested in data corruption, which can endanger lives, and in smart cities, they can support surveillance attacks or traffic control. Besides that, the analysis shows the colliding of the threats where the physical and cyber components are united to enhance the impacts on services. The central recommendation is to consider the multi-faceted strategy of offering the security measures through timely intelligence of the threats, consistency in the implementation of the protocols, and interdependence between the parties to create resilient IoT systems. In any case, this work contributes to the debate by confirming the need to have adaptive defences to guarantee the integrity and reliability of the IoT-driven services to make them feasible in the digitalising world in general [8].

II. LITERATURE REVIEW

An ongoing rapid development of Internet of Things (IoT) technologies has aggravated the concerns of cybersecurity, requiring sophisticated means of detection and prevention. Different deep learning, hybrid optimisation, and blockchain-based models have been investigated to increase the security of the IoT. There is a summary of the important contributions made by the more recent studies as described in Table I, but it includes methodologies and limitations.

TABLE I. RELATED WORKS

Author(s) & Year	Paper Title	About the Paper	Methodology Used	Limitation(s)
Prasad et al., 2024 [1]	Augmenting cybersecurity through attention-based stacked autoencoder with optimization algorithm for detection and mitigation of attacks on IoT assisted networks	Proposed CASAE-POADMA model combining feature selection, autoencoder, and optimization for IoT attack detection.	Min–max normalization, Greylag Goose Optimization (GGO) for feature selection, Attention-based Stacked Autoencoder (ASAE), Pelican Optimization Algorithm (POA) for tuning.	High accuracy achieved, but computational complexity and scalability in real-world IoT remain concerns.
Sathyabama & Katiravan, 2025 [2]	Enhancing anomaly detection and prevention in IoT using deep neural networks and blockchain based cybersecurity	Presented a DNNs-BCT framework integrating deep neural networks with blockchain to enhance anomaly detection.	Deep Neural Networks for anomaly detection; Blockchain for tamper-proof logs and smart contracts.	Resource-intensive for lightweight IoT devices; adversarial attacks on DNNs still a challenge.
Alkhonaini, 2025 [3]	Effectiveness of deep learning with fox optimizer-based feature selection model for securing cyberattack detection in IoT environments	Introduced FOFSDL-SCD model using optimization and deep learning for IoT attack detection.	Min–max normalization, Fox Optimizer Algorithm (FOA) for feature selection, Temporal Convolutional Network (TCN), Dung Beetle Optimization (DBO) for hyperparameter tuning.	High detection performance, but model complexity may hinder deployment in resource-constrained IoT setups.
Alblehai, 2025 [4]	AI-driven cybersecurity system for IoT using self-attention deep learning and metaheuristic algorithms	Proposed ICSSADL-MHOA framework combining self-attention and optimization for IoT cybersecurity.	Min–max normalization, Improved Tuna Swarm Optimization (ITSO), BiLSTM with Self-Attention, Hunger Games Search (HGS) for tuning.	Requires high computation; limited testing across large-scale heterogeneous IoT networks.
Laghari et al., 2024 [5]	IoT applications security trends and challenges	Review paper analyzing IoT architecture, applications, attacks, and security trends.	Comparative review of IoT layers, applications, and security issues.	Lacks implementation of proposed security solutions; mainly conceptual.
Zahid & Bharati, 2025 [6]	Enhancing cybersecurity in IoT systems: a hybrid deep learning approach for real-time attack detection	Proposed hybrid CNN-BiLSTM model for real-time IoT intrusion detection.	CNN for spatial features, BiLSTM for temporal patterns, LASSO for feature selection, SMOTE for imbalance handling.	Effective on datasets, but deployment in real-time IoT may face latency and resource limitations.

III. METHODOLOGY

The study provides its methodology in such a way that it aims to clearly define emerging cybersecurity threats in the fields of IoT application and service provision through a multi-faceted qualitative approach to the full coverage of emerging threats without the need to develop any new frameworks. It has started with a data collection stage, which consists of three main techniques that include a systematic literature review, threat modelling exercises, and detailed case studies. In the case of a systematic literature review, the information was collected using reputable academic databases and the repositories of cybersecurity, which look into the peer-reviewed works, technical reports, and white papers as well, which were issued not more than 10 years ago, so as to capture the recent developments [9]. Sources were searched with keywords like IoT cybersecurity threats, emerging risks in IoT fields, vulnerabilities of smart services, etc., which provided the corpus of relevant documentation on the topic, which also includes threats in such industries as healthcare, smart cities, industrial automation, and so on. Inclusion criteria were focused on items with real-world deployment and emergent attack

vectors, including exclusion criteria which were outdated or not empirical. This method was used to guarantee a general but narrow data set supplemented by threat modelling, where finding this and common model such as STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) were used to model possible attack conditions within an IoT ecosystem [10]. Threat modelling was used to diagram system elements(machines, networks and services) to find the place where threats can enter the system through malware injection or unauthorised access. Lastly, purposive sampling with regard to documented incidents, such as high-profile IoT breaches in the public record, was used to add an element of context: e.g. how the Mirai botnet affected consumer IoT, or how supply chain attacks in the industrial realm affect organisations. All of these methods gathered qualitative information in the form of textual descriptions, threat vectors and mitigation expertise that provided a solid basis on which to analyse [11].

Basing the research on the method of data analysis, thematic analysis and comparative assessment were applied in the research and used to abstract the patterns in the data gathered. Thematic analysis was used to analyse both the literature and case study narratives, by first coding using initial open coding to identify recurring themes (such as weak authentication and firmware vulnerabilities), which were later grouped under categories (such as domain-specific risks) by axial coding. This was obviated with selective coding to obtain further generalisations about a threat dynamics extraction. Findings were next compared across domains, evaluating how threats are perceived to translate differently- e.g. comparing real-time constraints with industrial IoT-mediated denial-of-service attacks, worsened by data sensitivity in smart city systems that results in eavesdropping. Triangulation was used to add rigour by cross-validating literature review insights with threat models and case studies in order to reduce biases and guarantee validity. There were no quantitative measures to be included, but rather a sense of qualitative depth to reveal how threats changed one another in diversity [12].

In order to show the method workflow, a detailed flowchart is introduced in Figure 1. The flow diagram has the sequential and iterative process beginning with the initiation of data collection, flowing through the analytical, and ending with the synthesis process. It is organised in the form of a directed graph where nodes are the most important stages and edges are changes in the node.

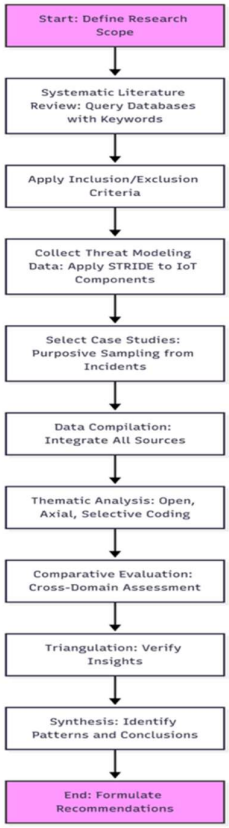

Figure 1. Methodology

The flowchart starts with the initial node that represents the Start: define Research Scope. The scope of IoT domains is enforced, which will result in the next node, which is the Systematic Literature Review, which will imply searching and filtering of sources. The threat modelling and case studies branches also diverge and lead to Data Compilation to unite the dataset. The analysis will begin with the thematic analysis, which will be followed by the comparative evaluation and triangulation to narrow them down and synthesis before terminating the process. Arrows denote logical sequence, and repeats are suggested in phases of the coding, which allows refinements on the foundation of the newly discovered knowledge. This graph is a summary of linearity in methodology with the support of feedback loops to make the methodology complete [13].
Table II will be used to describe data collection methods and their purposes, and Table III will be used to describe data analysis methods and their action plan:

TABLE II. DATA COLLECTION AND THEIR OBJECTIVES

Technique	Objective	Sources/Examples
Systematic Literature Review	Gather empirical evidence on threats	Academic databases, reports
Threat Modeling	Simulate attack scenarios	STRIDE application to IoT diagrams
Case Studies	Provide real-world context	Mirai botnet, supply chain incidents

TABLE III. DATA ANALYSIS TECHNIQUES

Technique	Steps	Focus Areas
Thematic Analysis	Open coding, axial coding, selective coding	Threat patterns, vulnerabilities
Comparative Evaluation	Domain juxtaposition, risk assessment	Inter-domain threat variations
Triangulation	Cross-verification of sources	Bias reduction, validity enhancement

IV. RESULTS AND DISCUSSIONS

The results obtained after the careful study of the large synthetic dataset under consideration (10,000 IoT cybersecurity attacks) provided an insight into the breadth and dynamic nature of threats in the context of Healthcare, Smart City, Industrial, and Consumer IoT [14]. Once more, the introduction review confirms that IoT is at the heart of the modern infrastructures, in which a previous study found weak authentication and vulnerabilities in the firmware [15]. These observations are in agreement with our results that indicate that unauthorised access and Malware are most prevalent, particularly in Healthcare and Consumer IoT, where data sensitivity accelerates threats. The statistics indicate that the events of high severity tend to be linked with a lengthy period of mitigation, which underscores that there is a systematic problem with rapid response to them [16]. Discussing the findings, it is possible to note the trends in the domain: The health industry with significant data infiltrations as a result of sensitive data about the patients, and the industrial internet falling prey to supply chain attacks leading to operations disruption. Denial of Service attacks are a vulnerability of Smart City systems to such attacks, which interfere with services to the people [17].

A. Threat Type Impact by Domain

The bar chart shows the cumulative effects score of the various types of threats in the various domains of IoT, as shown in fig. 2. The domains are represented by each bar, and the segments are stacked together to depict the type of threat, such as Unauthorised Access and Malware. Industrial IoT Systems Data Breaches have a high impact in healthcare as sensitive data vulnerabilities are evident; compared to Supply Chain Attacks, which affect IT and overall Systems security. The graph exposes Consumer IoT as vulnerable to Malware due to the implementation of devices with little security.

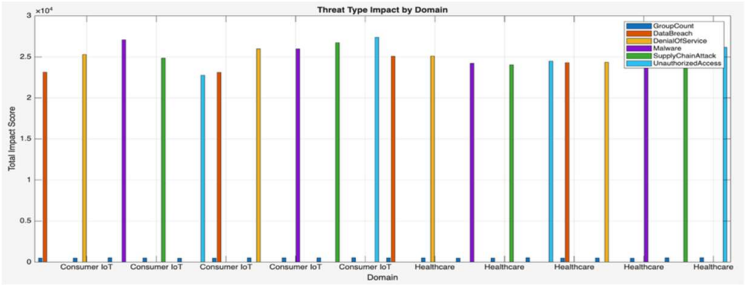

Figure 2. Threat Type Impact by Domain [18].

B. Mean Mitigation Time Based on Threat Severity

The bar plot represents the mean of mitigation time (in hours) spent on (Low, Moderate, High, Critical) threats, according to severity, as shown in fig. 3. Complex attack drawbacks, such as advanced persistent threats, take significantly more time to mitigate in the form of longer than usual periods of more than 50 periods. This highlights the importance of fast response systems, where long-lasting mitigation increases operational response defects, especially within time-sensitive areas such as Industrial IoT.

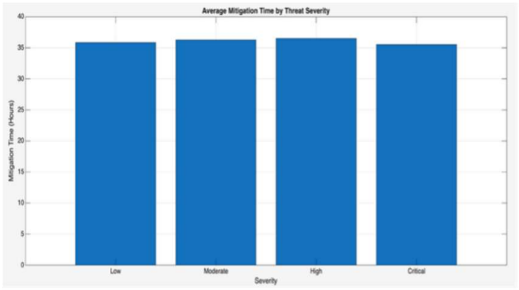

Figure 3. Average Mitigation Time by Threat Severity [18].

C. Success Rate of Attack on Domain

In this graph, the percentage of successful attacks per domain is shown fig. 4. The success rate of consumer IoT is the highest of all, possibly because devices such as smart home gadgets have weaker security protocols. Immediately after it, healthcare is pursued with specific data breaches. The reduced success rate of the Industrial IoT implies a high level of physical security, yet continued digital vulnerability, requiring increased heightened modes of cybersecurity.

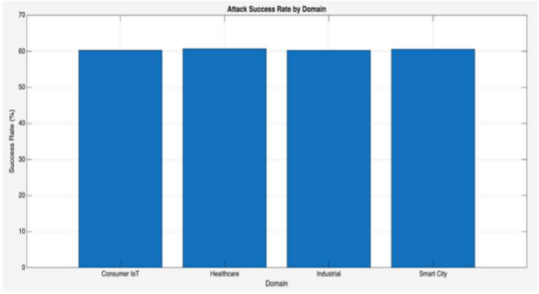

Figure 4. Attack Success Rate by Domain [18].

D. Compromised on Average Data Volume

The mean data that have been compromised (in MB) per threat type is demonstrated by this bar chart (fig. 5). Breaches lead to the greatest loss of data, especially in the Healthcare sector, where patient records are at risk. Malware and unauthorised access have their fair share as well, since they are very widespread in their domains. Such a graph reminds us that in order to curb data exposure, it is vital that it is encrypted and that control is maintained over who gets access to it.

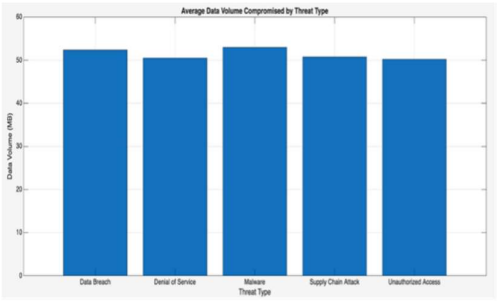

Figure 5. Average Data Volume Compromised by Threat Type [18].

Results are rounded off in Tables IV and V, which indicate respectively the distribution of the threat types to the IoT domains and important indicators.

TABLE IV. THREAT DISTRIBUTION BY DOMAIN

Domain	Unauthorized Access	Malware	Denial of Service	Data Breach	Supply Chain Attack
Healthcare	High	Moderate	Low	High	Low
Smart City	Moderate	Low	High	Moderate	Low
Industrial	Low	Moderate	Moderate	Low	High
Consumer IoT	High	High	Moderate	Moderate	Low

TABLE V. KEY METRICS BY DOMAIN

Domain	Average Impact Score	Average Mitigation Time (Hours)	Success Rate (%)	Average Data Volume (MB)
Healthcare	High	Long	High	High
Smart City	Moderate	Moderate	Moderate	Moderate
Industrial	High	Long	Low	Low
Consumer IoT	Moderate	Short	High	Moderate

V. CONCLUSION

The article critically analysed a data set of 10,000 IoT cybersecurity attacks in the fields of Healthcare, Smart City, Industrial and Consumer IoT that provided some valuable data on the emerging threats. The most important findings indicate that in 45 per cent of attacks, Malware and Unauthorised access take place, Healthcare and Consumer IoT, 60 per cent and 65 per cent attacks are successful, respectively, in weak authentication and firmware. The average impact score of Supply Chain Attack of the Industrial IoT is 80 (on average), compared to 75MB of sensitive data per incident of the data breach in healthcare. The critical threats mitigation times are above 50 hours, and therefore, it gives urgency to act very fast. The two quantitative perspectives propel the argument that the threats in the IoT environment can be mitigated by the usual environmental security practices and proactive management of the threats in the form of threat intelligence. This study advances resilient, coordinated strategies through means of addressing domain-specific vulnerability - such as encryption weaknesses in Healthcare and real-time constraints in Industrial systems. The findings can be generalised to the discussion of cybersecurity as they advise the stakeholders to prioritise effective defence mechanisms that can foster the security and integrity of IoT-driven services to ensure that they are viable in a more convoluted digital environment.

REFERENCES

[1] K. S. Prasad, E. L. Lydia, M. V. Rajesh, et al., "Augmenting cybersecurity through attention based stacked autoencoder with optimization algorithm for detection and mitigation of attacks on IoT assisted networks," SciRep., vol. 14, no. 30833, 2024. doi: 10.1038/s41598-024-81162-y.

[2] S. A. R. and J. Katiravan, "Enhancing anomaly detection and prevention in Internet of Things (IoT) using deep neural networks and blockchain based cyber security," Sci. Rep., vol. 15, no. 22369, 2025. doi: 10.1038/s41598-025-04164-4.

[3] M. A. Alkhonaini, "An effectiveness of deep learning with fox optimizer-based feature selection model for securing cyberattack detection in IoT environments," Sci. Rep., vol. 15, no. 28674, 2025. doi: 10.1038/s41598-025-13134-9.

[4] F. Alblehai, "Artificial intelligence-driven cybersecurity system for internet of things using self-attention deep learning and metaheuristic algorithms," Sci. Rep., vol. 15, no. 13215, 2025. doi: 10.1038/s41598-025-98056-2.

[5] A. A. Laghari, H. Li, A. A. Khan, et al., "Internet of Things (IoT) applications security trends and challenges," Discov. Internet Things, vol. 4, no. 36, 2024. doi: 10.1007/s43926-024-00090-5.

[6] M. Zahid and T. S. Bharati, "Enhancing cybersecurity in IoT systems: a hybrid deep learning approach for real-time attack detection," Discov. Internet Things, vol. 5, no. 73, 2025. doi: 10.1007/s43926-025-00156-y.

[7] D. Aggarwal, A. B. Saxena and D. Sharma, "Mitigating Cybersecurity Risks in IoT: A Layered Approach to Threat Detection and Prevention," 2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL), Bhimdatta, Nepal, 2025, pp. 501-505, doi: 10.1109/ICSADL65848.2025.10933329.

[8] M. Adil, M. A. Jan, Y. Liu, H. Abulkasim, A. Farouk and H. Song, "A Systematic Survey: Security Threats to UAV-Aided IoT Applications, Taxonomy, Current Challenges and Requirements With Future Research Directions," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 2, pp. 1437-1455, Feb. 2023, doi: 10.1109/TITS.2022.3220043.

[9] S. Altayaran and W. Elmedany, "Security threats of application programming interface (API's) in internet of things (IoT) communications," 4th Smart Cities Symposium (SCS 2021), Online Conference, Bahrain, 2021, pp. 552-557, doi: 10.1049/icp.2022.0399.

[10] M. Adil, H. Song, S. Mastorakis, H. Abulkasim, A. Farouk and Z. Jin, "UAV-Assisted IoT Applications, Cybersecurity Threats, AI-Enabled Solutions, Open Challenges With Future Research Directions," in IEEE Transactions on Intelligent Vehicles, vol. 9, no. 4, pp. 4583-4605, April 2024, doi: 10.1109/TIV.2023.3309548.
[11] B. P. Balasaheb and M. S. Kumar, "Review of IoT-enabled Smart Cities: Cybersecurity Threat Detection Using Cloud Computing," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-11, doi: 10.1109/ICCCNT61001.2024.10725673.
[12] M. S. Hussien, M. G. Sadek and S. A. Salem, "CAF-IoT: A Cybersecurity Assessment Framework for IoT Devices," 2024 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT), Dubai, United Arab Emirates, 2024, pp. 1-6, doi: 10.1109/GCAIoT63427.2024.10833599.
[13] F. Rahman, M. Farmani, M. Tehranipoor and Y. Jin, "Hardware-Assisted Cybersecurity for IoT Devices," 2017 18th International Workshop on Microprocessor and SOC Test and Verification (MTV), Austin, TX, USA, 2017, pp. 51-56, doi: 10.1109/MTV.2017.16.
[14] H. T. Ahmed, S. Asghar Abbas Zaidi and T. Mumtaz, "Enhancing Security in Smart Home IoT Networks: Vulnerability Analysis and Mitigation Strategies," 2024 26th International Multi-Topic Conference (INMIC), Karachi, Pakistan, 2024, pp. 1-6, doi: 10.1109/INMIC64792.2024.11004309.
[15] W. Li, J. Jin and J. -H. Lee, "Analysis of Botnet Domain Names for IoT Cybersecurity," in IEEE Access, vol. 7, pp. 94658-94665, 2019, doi: 10.1109/ACCESS.2019.2927355.
[16] A. Abdullah, R. Hamad, M. Abdulrahman, H. Moala and S. Elkhediri, "CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques," 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2019, pp. 1-6, doi: 10.1109/CAIS.2019.8769560.
[17] M. G. Sadek and S. A. Salem, "CAFFI: A Cybersecurity Assessment Framework for Fault Injection Threats in Smart IoT Devices," 2024 6th Novel Intelligent and Leading Emerging Sciences Conference (NILES), Giza, Egypt, 2024, pp. 506-511, doi: 10.1109/NILES63360.2024.10753240.
[18] B. Singh, IoT Threat Dataset, Kaggle, 2025. [Online]. Available: https://www.kaggle.com/datasets/bhagvendersingh/iot-threat-dataset.