KARYA ILHAM PUBLISHING
CONNECTING MINDS, BRIDGING IDEAS, INSPIRING READERS

International Journal of Advanced Research in Computational Thinking and Data Science

Journal homepage:
https://karyailham.com.my/index.php/ctds/index
ISSN: 3030-5225

CyberShield Framework: Attacks and Defense Modelling for Cybersecurity in Internet of Things (IoT)

Moustafa Abdelrahman Mahmoud Ahmed[1], Syahril Anuar Idris[1], Nur Arzilawati Md Yunus[2,*], Fazlina Mohd Ali[3], Hazrina Sofian[4]

[1] University Malaysia of Computer Science and Engineering, 46200 Petaling Jaya, Selangor, Malaysia
[2] Department of Communication Technology and Network, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Selangor, Malaysia
[3] Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Selangor, Malaysia
[4] Department of Software Engineering, College of Computer and Cyber Sciences, University of Prince Mugrin, Kingdom of Saudi Arabia

ARTICLE INFO

Article history:
Received 29 October 2024
Received in revised form 20 November 2024
Accepted 9 December 2024
Available online 31 December 2024

Keywords:

Keywords; Internet of Things; cybersecurity; threats, security; attacks

ABSTRACT

The rapid emergence of Internet of Things (IoT) devices has ushered in an era of unprecedented connectivity and convenience, but it has also brought forth an array of cybersecurity challenges. This research deals with the multifaceted realm of cybersecurity threats on the Internet of Things (IoT) landscape. The vulnerabilities inherent in this ever-expanding ecosystem have become increasingly evident as IoT devices permeate every facet of our daily lives. In this paper, we review the various security threats that IoT deployments face, ranging from unauthorized access and data breaches to device vulnerabilities, physical attacks, and the pressing concerns surrounding user privacy. As the IoT continues to reshape our digital landscape, understanding and mitigating cybersecurity threats, in this paper we propose the attack and defense modelling framework to ensuring interconnected devices and systems' security, privacy, and resilience. This research serves as a foundational overview, urging stakeholders to prioritize IoT security in a world increasingly reliant on the promise of a hyper-connected future. By thoroughly synthesizing current knowledge in IoT, this research equips readers with a holistic understanding of IoT cybersecurity threats, enabling stakeholders to make informed decisions in a connected world. In the face of escalating risks, this research serves as a vital resource for academia, industry professionals, policymakers, and cybersecurity practitioners, all committed to fortifying the integrity and resilience of IoT ecosystems.

1. Introduction

The Internet of Things (IoT) has emerged as a transformative force, weaving a seamless web of connectivity across our increasingly digitized world. With promises of enhanced convenience, efficiency, and productivity, IoT technologies have penetrated diverse domains, from smart homes

* *Corresponding author.*
E-mail address: nurarzilawati@upm.edu.my

https://doi.org/10.37934/ctds.4.1.3039a

and healthcare to industrial automation and urban infrastructure [1]. However, this digital ubiquity has not come without a cost. The very connectivity that underpins IoT's promise has also introduced a host of formidable cybersecurity threats and vulnerabilities that challenge the security and privacy of IoT ecosystems. As our world becomes increasingly interconnected, the need to address these threats has never been more critical. The threats to IoT security are diverse and continuously evolving. They encompass a wide range of vulnerabilities and attack vectors, including unauthorized access to devices, data breaches, exploitation of device vulnerabilities, physical attacks on IoT hardware, and the erosion of user privacy [2]. The rapid expansion of the IoT has introduced a wide range of cybersecurity vulnerabilities and threats, including but not limited to unauthorized access, data breaches, device hijacking, and distributed denial-of-service (DDoS) attacks. These threats can lead to severe consequences, ranging from the compromise of personal data to the disruption of essential services. Despite the growing awareness of these issues, there remains a pressing need to identify and categorise the cyber-attacks targeting IoT devices and networks [3]. As IoT devices proliferate, they become prime targets for cyber-attacks due to their often-limited computational capabilities and lack of standardized security protocols. This technological change raises new threats and security attacks that produce new and complex cybersecurity scenarios with large volumes of data and different attack vectors that can exceed the cognitive skills of security analysts [4]. Traditional cybersecurity models, designed for conventional networks, are insufficient to address the unique challenges posed by IoT environments. Current security practices are often inadequate or inconsistent across devices and networks, leading to potential risks for both individuals and organizations [3]. The aim of this research is to identify and propose practical guidelines and best practices to enhance IoT security, focusing on key areas such as device authentication, data encryption, secure communication protocols, network segmentation, and firmware integrity. These guidelines will serve to minimize vulnerabilities and ensure a secure IoT environment, balancing security needs with the performance constraints of IoT devices.

While significant strides have been made in identifying IoT-related cybersecurity threats, a clear, systematic framework for categorizing and mitigating these threats remains underdeveloped. Existing security models often fall short in addressing the unique and evolving nature of IoT environments due to limited computational resources, the absence of standardized protocols, and diverse attack vectors. Furthermore, traditional security practices are insufficient for handling the large-scale, real-time data generated by IoT devices, which can overwhelm current security systems and analysts. This research seeks to bridge this gap by proposing the framework tailored specifically for IoT environments, focusing on areas such as device authentication, data encryption, secure communication protocols, network segmentation, and firmware integrity.

2. Literature Review

The Internet of Things (IoT) devices, often characterized by limited resources, are susceptible to a variety of cyberattacks. Studies have documented attacks such as Distributed Denial of Service (DDoS), data interception, and spoofing [5]. The vulnerability of IoT devices poses significant security challenges. The technology-facilitated abuse through IoT devices has a substantial impact on intimate partner violence (IPV) [6]. Improper device updates, inadequate security protocols, user unawareness, and lack of active device monitoring contribute to the challenges faced by IoT [7]. The limitations of traditional security models in IoT environments necessitate lightweight security protocols and decentralized approaches like blockchain. A framework for smart government performance emphasizes the importance of IoT-enabled dynamic capabilities and public policies [8]. The automation of cognitive tasks in cyber operations, with human involvement for validation and

decision-making, is crucial. A new IoT model aims to enhance user security and privacy [9]. Advanced deep learning techniques, such as LSTM modules, are employed to detect cyber-attacks in IoT systems [10]. Current defence strategies for IoT, including anomaly detection, machine learning-based intrusion detection systems, and encryption techniques, often face challenges in scalability and resource efficiency [7]. An open-source solution for simulating cyber infrastructures and IoT scenarios, with a focus on edge applications, is available [11]. A brief overview of deep learning methods used in cybersecurity, such as deep belief networks, generative adversarial networks, and recurrent neural networks, is provided [12]. A blockchain-based framework for an open-bid auction system addresses privacy and security concerns using various cryptographic primitives [13]. Developing protection mechanisms against IoT attacks is crucial, as attackers seek vulnerabilities in networks to target connected devices. A cloud-enabled IoT environment in AWS implements the top layer, with security protocols and critical management sessions ensuring user privacy across different layers [14].

2. Cybersecurity Threats in IoT

Security threats are main critical challenges for the devices in an IoT environment such as in industrial [3], maritime [15], government [8] as shown in Figure 1. The hyper-connectivity generated by IoT networks coupled with limited default security in IoT devices increases security risks that can jeopardize the operations of cities, hospitals, and organizations [16]. Security is central for IoT systems to protect sensitive data and infrastructure, whilst security issues have become increasingly expensive, in Industrial Internet of Things (IoT) domains [17] IoT-based critical infrastructures are an appealing target for cybercriminals. Such distinctive infrastructures are increasingly sensitive to cyber vulnerabilities and subject to many cyberattacks [18]. They contain communication systems that can lead to national security deficits, disruption of public order, loss of life or large-scale economic damage when the confidentiality, integrity, or availability of the communication is broken down. These huge systems may be vulnerable to cyber-attacks [5]. Major challenges are security since the devices are online hence making the smart grid vulnerable to significant attacks [4]. Improper device updates, lack of efficient and robust security protocols, user unawareness, and famous active device monitoring are among the challenges that IoT is facing [7]. The common vulnerabilities notable in IoT include the security, privacy, and data protection concerns [9]. This technological change rise to new threats and security attacks that produce new and complex cybersecurity scenarios with large volumes of data and different attack vectors that can exceeded the cognitive skills of security analysts [4]. Analysis of those data sources is still a big challenge for reducing high dimensional space and selecting important features and observations from different data sources [19]. The technology-facilitated abuse, so-called “tech abuse,” through phones, trackers, and other emerging innovations, has a substantial impact on the nature of intimate partner violence (IPV) [6].

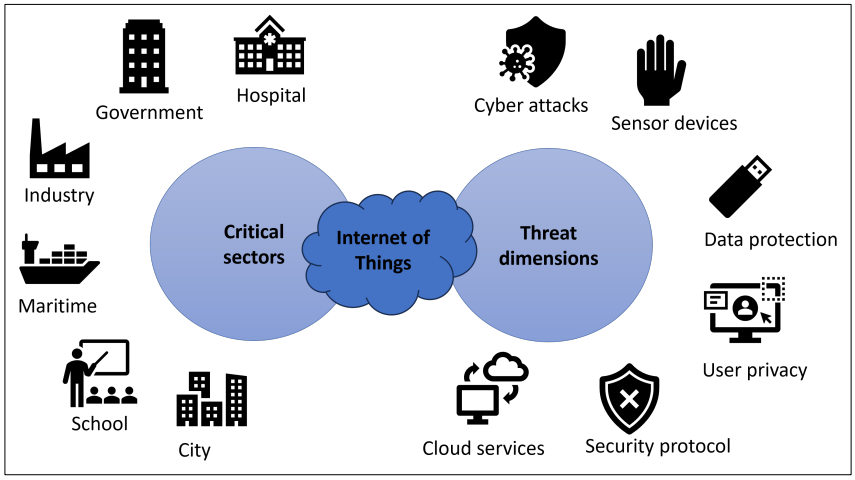

Fig. 1. Critical sectors and threat dimensions in IoT environments

User privacy is another concern in IoT because the electronic environment enables the collection of personal data [13]. The cybersecurity aspects define an assessment model of cybersecurity maturity of IoT solutions to develop smart city applications [20]. The network traffic of a smart city via loT systems is growing exponentially and introducing new cybersecurity challenges since these loT devices are being connected to sensors that are directly connected to massive cloud servers [21]. Security properties of such distributed control systems are typically only verified empirically during development and after system deployment [22]. IoT relies on utilizing the Internet to operate it is vulnerable to Cyber-attacks if security is not taken into consideration [23]. Cybersecurity and highlights the need to address the possible threats targeting (various pillars of) industry 4.0. [24].

Fig. 2. Industry 4.0 pillars

Therefore, needs the cybersecurity awareness within industrial contexts based on the IoT paradigm to defend critical systems and sensitive data against emerging security threats and attacks [25][11]. Growing numbers of cyberattacks show that current security solutions and technologies do not provide effective safeguard against modern attacks [26]. Thus, we need to identify the possible attacks of digital virtual assets and timely accurate assessment the risks by securing these devices and systems are compounded by the scale and diversity of deployment, the fast-paced cyberthreat landscape, and many other factors [27,28].

3. Issues in Previous Works

Cybersecurity on the Internet of Things (IoT) is a critical and evolving concern due to the proliferation of connected devices in our homes, workplaces, and industries. IoT security is essential because these devices often handle sensitive data and can be vulnerable to various cyber threats. Table 1 review the cybersecurity threats on internet of things in previous works.

Table 1
Review of cybersecurity threats on internet of things

Ref.	Previous work	Results
[3]	CNN-based approach for anomaly-based intrusion detection systems (IDS) that takes advantage of IoT's power, providing qualities to efficiently examine whole traffic across the IoT.	Convolutional neural network (CNN) model improves the IoT network's performance and security and able to detect any possible intrusion and abnormal traffic behavior.
[8]	Framework for IoT-enabled smart government performance	The results show evidence of forward-thinking initiatives with the developing IoT-enabled dynamic capabilities capable of addressing some of the problems faced by the U.S.
[11]	Open-source solution for simulating cyber infrastructures and reproducing realistic Internet of Things (IoT) scenarios, with specific focus on Edge applications.	The Cyber range is fully working and can be used as a valid basis for building more articulated and challenging IoT-Edge training exercises, as well as validate solutions that can be used to prevent, detect, mitigate, recovery, and evaluate the attack impact.
[5]	The application of IoT as an enabling technology for the smart grid.	The use of the IoT is shown to improve the existing grid networks to facilitate better monitoring and control of the power grids.
[4]	The automation process in the execution of cognitive tasks defined in the cyber operations processes and includes the analyst as the central axis in the processes of validation and decision making.	The security cognitive model proposal in this work integrates technological solutions with cognitive process and control techniques that allows to provide a complete vision of the cybersecurity situation awareness.
[6]	The risks and harms posed to IPV victims/survivors from the burgeoning Internet of Things (IoT) environment.	Vividly illustrated why IPV research needs to engage with the development of digital devices and keep a tab on emerging technologies such as IoT.
[24]	Investigating the possible cyber-attacks targeting 4 layers of IIoT.	Discussed various pillars of IR 4.0, including autonomous robots, simulation, cyber-security, IIoT, horizontal and vertical integration, augmented reality, etc
[9]	New IoT model that can enhance the security and privacy of the users of the IoT.	Model for the IoT architecture proves powerful in addressing the security vulnerabilities that organizations and businesses face in their daily operations
[19]	New testbed for an IIoT network that was utilized for creating new datasets called TON_IoT that collected Telemetry data, Operating systems data and Network data.	New testbeds for IoT networks, datasets, and their analysis for validating cybersecurity applications
[12]	Deep learning methods which is used in cybersecurity, including deep belief networks, generative adversarial networks, recurrent neural networks, and others.	Illustrates that the standard datasets are very important to advancing DL in the cybersecurity domain
[29]	Decision Support System (DSS)-based farming management that utilizes widespread IoT sensors and wireless connectivity to enable automated detection and optimization of resources.	Identified fifty-eight cyber security threats which need to be controlled for a thriving smart farming eco-system.
[30]	Structured approach to mitigate cybersecurity risks on the Internet of Things (IoT)	Current approaches do not provide a suitable strategy for IoT cybersecurity certification.

[20]	Model based on risk levels to evaluate the IoT cybersecurity maturity in a smart city.	Cognitive security techniques, it would be possible to assess cybersecurity risk levels in the face of complexity, diversity, and large volumes of data in IoT ecosystems
[22]	Novel modelling framework for the security verification of distributed industrial control systems, with the goal of moving towards early design stage formal verification.	Framework can be used at an early design stage to eliminate potential attacks and security threats.
[23]	Provide the different classifications of attacks that an attacker can launch against these devices and mentions methods of mitigating such attacks.	This invention has fueled the transition of the industrial sector to Smart Industry/Industry 4.0 where large production plants can generate products by utilizing the process of automation.
[15]	The proneness of the digital transformation is analyzed regarding the use of internet of things (IoT) devices, modern security frameworks for ships, and sensors and devices used in modern ships.	The cyber security threats for the maritime industry regarding the devices used for sensing, communication, navigation, and emergency response in case of distress
[21]	Anomaly Detection IoT (AD-IoT) system, which is an intelligent anomaly detection based on Random Forest machine learning algorithm.	AD-IoT can significantly detect malicious behavior using anomalies based on machine learning through the evaluation of the UNSW-NB 15 dataset to detect the binary labeled classification before distributing on fog nodes.
[27]	Selection algorithm based on the "Designated + Random" mode by hierarchical division (HD-NSA), which can efficiently generate high-performance immune detectors to identify attack risks	Detection algorithm can detect attacks faster and more accurately, compared with V-Detector and BIORV-NS.
[10]	Integrates a set of long short-term memory (LSTM) modules using advanced deep learning into an ensemble of detector to detect the cyber-attacks against IoT systems.	Integrated an ensemble of LSTM deep model and aggregated their outputs to achieve enhanced robustness.
[28]	Precautions against these attacks and to develop protection methods.	Using appropriate IDS techniques is an important cyber-security aspect as it helps, taking countermeasures in advance, also it enables developing a predictive and proactive cyber-security posture for IoT-based critical infrastructures.
[7]	Cloud-enabled IoT environment in AWS to implement the top layer (the cloud) to ensure the privacy of the users' information.	Implemented security certificates to allow data transfer between the layers of the proposed Cloud/Edge enabled IoT model.
[16]	Process of hardening and vulnerability analysis to reduce the attack surface and improve the security level of the IoT solution.	The contributions of the research analyzed allow the risks to be determined by means of standards proposed by international organizations, such as ISO, OWASP, and NIST.
[18]	Security requirements and some realistic recommendations to enhance cybersecurity solutions.	a new taxonomy of modern cyberattacks impacting cyber critical infrastructure, and some realistic recommendations and best practices to enhance cybersecurity solutions.
[24]	New cybersecurity technologies/ applications present improvements for IoT security management.	Organizations need to keep up with the development of technologies to respond appropriately to cybersecurity threats.
[31]	New lightweight algorithm named enhanced 3D RECTANGLE, designed to deliver robust security for IoT applications and optimized for cell phones with minimal memory usage, low power consumption, and efficient performance.	improves the RECTANGLE algorithm through the use of a composite S-Box and 3D shift rotation techniques
[32]	Application of information technology using multiple devices such as smartphone devices and personal computers to farmers and herbal plant	The modules providing the users to access accurate, transparent and accountable reports regarding to national

	entrepreneurs, to improve the conditions and capabilities of processing herbal plants into a profitable business in terms of costs and technological efficiency.	health requirements at the provincial government of Indonesia

4. CyberShield Framework: Attacks and Defense Modelling for Cybersecurity in IoT

The Internet of Things (IoT) has embarked on a transformative journey that promises to reshape how we live, work, and interact with the digital world. As IoT technologies proliferate across diverse domains, the benefits of enhanced connectivity, automation, and data driven. Critical sectors in IoT environments include healthcare, transportation, energy, manufacturing, smart cities, and agriculture, each facing unique threats such as data breaches, vehicle hacking, infrastructure attacks, and supply chain vulnerabilities. The key threat dimensions encompass data security, device vulnerabilities, network security, supply chain risks, privacy concerns, and physical security. Understanding these sectors and their associated threats is essential for developing targeted security strategies to protect IoT systems and data. In this section we propose the defence modelling for cybersecurity threats in the IoT framework as shown in Figure 3 include implementing robust authentication and access control measures, such as multi-factor authentication and role-based access, to ensure that only authorized users can interact with devices. Regular firmware updates and patches should be enforced to address vulnerabilities promptly, while strong encryption protocols safeguard data in transit and at rest. Network segmentation can limit the potential impact of a breach, and intrusion detection systems (IDS) can monitor traffic for anomalies. Additionally, fostering a security-aware culture through user education and incident response planning is essential for maintaining resilience against evolving threats in IoT environments. Implementing these strategies can significantly enhance the security posture of IoT systems and reduce the likelihood of successful cyberattacks.

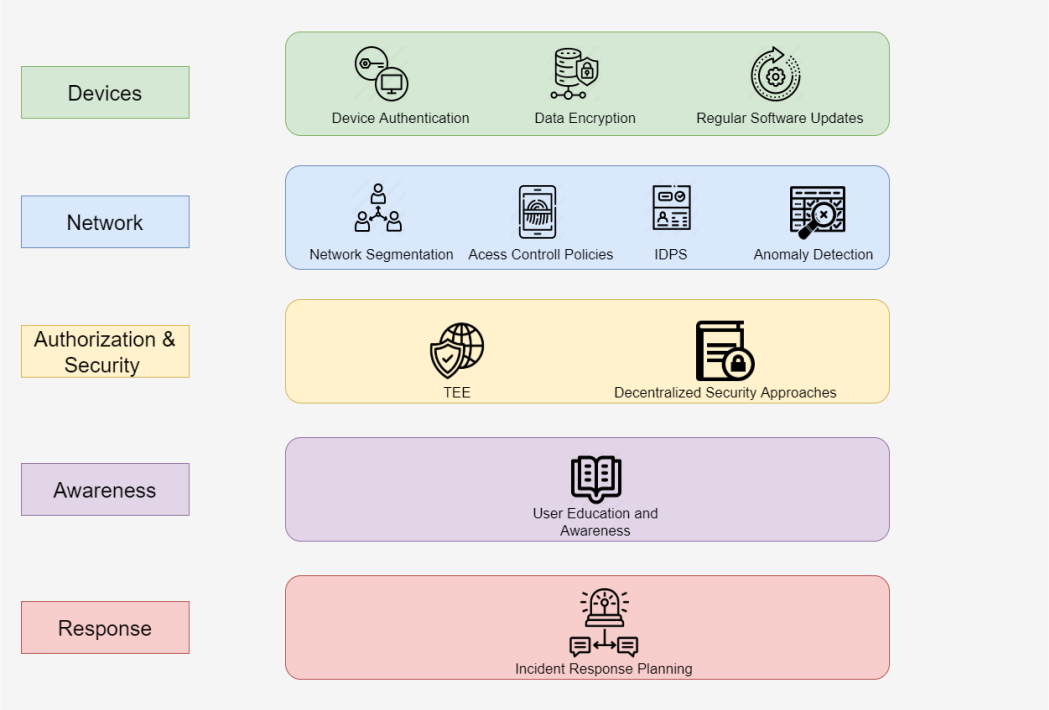

Fig. 3. CyberShield Framework: Attacks and Defense Modelling for Cybersecurity in IoT

i. Device Authentication
   Implement strong authentication mechanisms for devices to prevent unauthorized access. Use techniques like digital certificates, public key infrastructure (PKI), or two-factor authentication (2FA).
ii. Data Encryption
   Encrypt data at rest and in transit to protect sensitive information from interception. Use robust encryption standards (e.g., AES, TLS) to secure communications.
iii. Regular Software Updates
   Ensure that IoT devices receive regular firmware and software updates to patch vulnerabilities. Automate updates, when possible, to minimize security risks.
iv. Network Segmentation
   Use network segmentation to isolate IoT devices from critical systems. This can limit the impact of a breach and reduce the attack surface.
v. Access Control Policies
   Implement strict access control policies that limit user privileges based on the principle of least privilege (PoLP). Regularly review and update access rights.
vi. Intrusion Detection and Prevention Systems (IDPS)
   Deploy IDPS to monitor network traffic and detect suspicious activities in real-time. Use machine learning algorithms to enhance detection capabilities.
vii. Anomaly Detection
   Utilize machine learning techniques to establish baselines of normal behavior for IoT devices and detect anomalies that may indicate a security breach.
viii. Secure Boot and Trusted Execution Environments (TEE)
   Use secure boot processes to ensure that only authorized firmware is loaded during device startup. TEEs can protect sensitive data and code from unauthorized access.
ix. User Education and Awareness
   Educate users about IoT security risks and best practices. Awareness can help mitigate risks associated with social engineering and poor security hygiene.
x. Incident Response Planning
   Develop and maintain an incident response plan specifically tailored for IoT environments. This should include procedures for detection, containment, eradication, and recovery.
xi. Decentralized Security Approaches
   Explore blockchain-based solutions for device authentication, data integrity, and secure communications, enhancing resilience against attacks.

5. Conclusions

The Internet of Things (IoT) has embarked on a transformative journey that promises to reshape how we live, work, and interact with the digital world. As IoT technologies proliferate across diverse domains, the benefits of enhanced connectivity, automation, and data-driven insights are undeniable. This research aims to contribute to the field of IoT cybersecurity by providing a comprehensive framework for understanding and mitigating cyber threats specific to IoT environments. By focusing on attack categorization and defence modelling, the study will address the critical need for tailored security solutions in the rapidly expanding IoT ecosystem. The findings are expected to offer valuable insights for researchers, developers, and policymakers in enhancing the security posture of IoT deployments. The urgency of addressing these threats cannot be overstated, as recent incidents and cyberattacks have illustrated the real-world consequences of IoT

vulnerabilities. IoT cybersecurity is not a static destination but an ongoing journey demanding perpetual vigilance and adaptability. The knowledge and insights shared in this research aim to equip stakeholders from academia, industry, and policymaking with the tools and understanding needed to fortify the integrity and resilience of IoT ecosystems. In the interconnected world we envision, where the Internet of Things plays a vital role, we must stand together to safeguard the promise of a secure connected future. The key points discussed in the review paper on IoT cybersecurity threats emphasize the need for proactive measures and collaboration in addressing these challenges.

Acknowledgement
This research was not funded by any grant.

References

[1] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." *Computer networks* 54, no. 15 (2010): 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

[2] Mohd Ali, Fazlina, Nur Arzilawati Md Yunus, Nur Nabila Mohamed, Marizuana Mat Daud, and Elankovan A. Sundararajan. "A Systematic Mapping: Exploring Internet of Everything Technologies and Innovations." *Symmetry* 15, no. 11 (2023): 1964. https://doi.org/10.3390/sym15111964

[3] Saba, Tanzila, Amjad Rehman, Tariq Sadad, Hoshang Kolivand, and Saeed Ali Bahaj. "Anomaly-based intrusion detection system for IoT networks through deep learning model." *Computers and Electrical Engineering* 99 (2022): 107810. https://doi.org/10.1016/j.compeleceng.2022.107810

[4] Andrade, Roberto O., and Sang Guun Yoo. "Cognitive security: A comprehensive study of cognitive science in cybersecurity." *Journal of Information Security and Applications* 48 (2019): 102352. https://doi.org/10.1016/j.jisa.2019.06.008

[5] Kimani, Kenneth, Vitalice Oduol, and Kibet Langat. "Cyber security challenges for IoT-based smart grid networks." *International journal of critical infrastructure protection* 25 (2019): 36-49. https://doi.org/10.1016/j.ijcip.2019.01.001

[6] Slupska, Julia, and Leonie Maria Tanczer. "Threat modeling intimate partner violence: Tech abuse as a cybersecurity challenge in the internet of things." In *The Emerald international handbook of technology-facilitated violence and abuse*, pp. 663-688. Emerald Publishing Limited, 2021. https://doi.org/10.1108/978-1-83982-848-520211049

[7] Tawalbeh, Lo'ai, Fadi Muheidat, Mais Tawalbeh, and Muhannad Quwaider. "IoT Privacy and security: Challenges and solutions." *Applied Sciences* 10, no. 12 (2020): 4102. https://doi.org/10.3390/app10124102

[8] A. T. Chatfield and C. G. Reddick, "A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity Chatfield, Akemi Takeoka, and Christopher G. Reddick. "A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in US federal government." *Government Information Quarterly* 36, no. 2 (2019): 346-357. https://doi.org/10.1016/j.giq.2018.09.007

[9] Lee, Calvin, and Gouher Ahmed. "Improving IoT privacy, data protection and security concerns." *International Journal of Technology, Innovation and Management (IJTIM)* 1, no. 1 (2021): 18-33. https://doi.org/10.54489/ijtim.v1i1.12

[10] Saharkhizan, Mahdis, Amin Azmoodeh, Ali Dehghantanha, Kim-Kwang Raymond Choo, and Reza M. Parizi. "An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic." *IEEE Internet of Things Journal* 7, no. 9 (2020): 8852-8859. https://doi.org/10.1109/JIOT.2020.2996425

[11] Ficco, Massimo, and Francesco Palmieri. "Leaf: An open-source cybersecurity training platform for realistic edge-IoT scenarios." *Journal of Systems Architecture* 97 (2019): 107-129. https://doi.org/10.1016/j.sysarc.2019.04.004

[12] Podder, Prajoy, Subrato Bharati, M. Mondal, Pinto Kumar Paul, and Utku Kose. "Artificial neural network for cybersecurity: A comprehensive review." *arXiv preprint arXiv:2107.01185* (2021).

[13] Sarfaraz, Aaliya, Ripon K. Chakrabortty, and Daryl L. Essam. "A tree structure-based improved blockchain framework for a secure online bidding system." *Computers & Security* 102 (2021): 102147. https://doi.org/10.1016/j.cose.2020.102147

[14] Shah, Yash, and Shamik Sengupta. "A survey on Classification of Cyber-attacks on IoT and IIoT devices." In *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pp. 0406-0413. IEEE, 2020. https://doi.org/10.1109/UEMCON51285.2020.9298138

[15] Ashraf, Imran, Yongwan Park, Soojung Hur, Sung Won Kim, Roobaea Alroobaea, Yousaf Bin Zikria, and Summera Nosheen. "A survey on cyber security threats in IoT-enabled maritime industry." *IEEE Transactions on Intelligent Transportation Systems* 24, no. 2 (2022): 2677-2690. https://doi.org/10.1109/TITS.2022.3164678

[16] Echeverría, Aarón, Cristhian Cevallos, Ivan Ortiz-Garces, and Roberto O. Andrade. "Cybersecurity model based on hardening for secure internet of things implementation." *Applied Sciences* 11, no. 7 (2021): 3260. https://doi.org/10.3390/app11073260
[17] Raimundo, Ricardo Jorge, and Albérico Travassos Rosário. "Cybersecurity in the internet of things in industrial management." *Applied Sciences* 12, no. 3 (2022): 1598. https://doi.org/10.3390/app12031598
[18] 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. https://doi.org/10.3390/app11104580
[19] Moustafa, Nour. "New generations of internet of things datasets for cybersecurity applications based machine learning: TON_IoT datasets." In *Proceedings of the eResearch Australasia Conference, Brisbane, Australia*, pp. 21-25. 2019.
[20] Andrade, Roberto Omar, Sang Guun Yoo, Luis Tello-Oquendo, and Iván Ortiz-Garcés. "A comprehensive study of the IoT cybersecurity in smart cities." *IEEE Access* 8 (2020): 228922-228941. https://doi.org/10.1109/ACCESS.2020.3046442
[21] Chakrabarti, S. "IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC): 7th-9th January, 2019." *University of Nevada, Las Vegas, NV, USA* (2019).
[22] Kulik, Tomas, Peter WV Tran-Jørgensen, Jalil Boudjadar, and Carl Schultz. "A framework for threat-driven cyber security verification of iot systems." In *2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, pp. 89-97. IEEE, 2018. https://doi.org/10.1109/ICSTW.2018.00033
[23] R. Paul. "Institute of Electrical and Electronics Engineers. New York Section, Institute of Electrical and Electronics Engineers. Region 1, IEEE-USA, and Institute of Electrical and Electronics Engineers." In *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) :* 28th- 31st October 2020. New York, USA. virtual conference.
[24] Jhanjhi, N. Z., Mamoona Humayun, and Saleh N. Almuayqil. "Cyber security and privacy issues in industrial internet of things." *Computer Systems Science & Engineering* 37, no. 3 (2021). https://doi.org/10.32604/csse.2021.015206
[25] Corallo, Angelo, Mariangela Lazoi, Marianna Lezzi, and Angela Luperto. "Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review." *Computers in Industry* 137 (2022): 103614. https://doi.org/10.1016/j.compind.2022.103614[23
[26] Nazir, Anjum, and Rizwan Ahmed Khan. "A novel combinatorial optimization based feature selection method for network intrusion detection." *Computers & Security* 102 (2021): 102164. https://doi.org/10.1016/j.cose.2020.102164
[27] He, Junjiang, Tao Li, Beibei Li, Xiaolong Lan, Zhiyong Li, and Yunpeng Wang. "An immune-based risk assessment method for digital virtual assets." *Computers & Security* 102 (2021): 102134. https://doi.org/10.1016/j.cose.2020.102134
[28] Das, Resul, and Muhammet Zekeriya Gündüz. "Analysis of cyber-attacks in IoT-based critical infrastructures." *International Journal of Information Security Science* 8, no. 4 (2019): 122-133.
[29] Al Asif, Md Rashid, Khondokar Fida Hasan, Md Zahidul Islam, and Rahamatullah Khondoker. "STRIDE-based cyber security threat modeling for IoT-enabled precision agriculture systems." In *2021 3rd International Conference on Sustainable Technologies for Industry 4.0 (STI)*, pp. 1-6. IEEE, 2021. https://doi.org/10.1109/STI53101.2021.9732597
[30] Matheu, Sara N., Jose L. Hernandez-Ramos, Antonio F. Skarmeta, and Gianmarco Baldini. "A survey of cybersecurity certification for the internet of things." *ACM Computing Surveys (CSUR)* 53, no. 6 (2020): 1-36. https://doi.org/10.1145/3410160
[31] Ali, Tasnuva, Azni Haslizan Ab Halim, and Nur Hafiza Zakaria. "3D Lightweight Cryptosystem Design for IoT Applications Based on Composite S-Box." *International Journal of Computational Thinking and Data Science* 3, no. 1 (2024): 40-54. https://doi.org/10.37934/ctds.3.1.4054
[32] Noviarini, Diena, Osly Usman, and Akhmad Yamani. "Smart Herbs IoT." *Semarak International Journal of Applied Sciences and Engineering Technology* 3, no. 1 (2024): 1-6.