Engineering Innovations
ISSN: 2813-1002, Vol. 16, pp 107-114
doi:10.4028/p-2GUuyA

Submitted: 2025-04-21
Revised: 2025-08-06
Accepted: 2025-08-09
Online: 2026-01-07

IoT Security: Solutions to Mitigate Attacks

Andrea Gisselle Menjivar[1,a]
Florida International University, Miami, Florida
[a]amenj003@fiu.edu

Keywords: IoT, Security, Mitigation.

Abstract. The Internet of Things (IoT) is one of the most transformative technologies in recent years, offering unprecedented connectivity and functionality across a wide range of industries. However, like all internet-connected systems, IoT devices are vulnerable to significant security threats. These vulnerabilities pose serious risks to both residential and industrial environments, as attackers can exploit them to compromise privacy, disrupt services, or cause physical harm. Traditional cybersecurity approaches are often impractical for IoT devices due to their resource constraints and unique architectures. This paper begins by defining IoT devices and illustrating the scale of the security challenges they face. Then it explores the three fundamental pillars of IoT security, confidentiality, integrity, and availability, highlighting their importance and how current techniques aim to uphold them. Finally, the article reviews various mitigation strategies proposed in the literature to provide a clearer picture of the evolving threat landscape and the measures needed to protect user trust and ensure the safe adoption of IoT technologies.

I. Introduction

Over the years, the transformative technology known as the Internet of Things (IoT) has significantly changed how we interact with the world around us. IoT is a constantly evolving technology driven by the increasing need for people to live in a more interconnected world. It enables the connection of realworld objects to digital platforms, allowing users to monitor and control them remotely [1]. A simple way to understand IoT is to consider it as any device capable of collecting data and transmitting it to the cloud through an internet connection. This allows users to access data from anywhere. IoT-based systems automate, integrate, and manage processes through sensors and communication technologies [2]. This revolutionary technology is advancing telecommunications and enhancing quality of life globally through its wide range of applications. In manufacturing, it enables increased efficiency and predictive maintenance; in transportation, it improves logistics, real-time tracking, and safety measures; in the energy sector, it optimizes resource use, monitors equipment performance, and improves overall operational efficiency; in retail, it streamlines inventory management, personalizes customer experiences, and provides real-time analytics. IoT is also crucial in the development of smart cities, healthcare systems, and supply chains, among others. By playing a key role across multiple industries, IoT has substantial potential for driving global economic growth. Today, there are approximately 26.66 billion IoT devices in use worldwide, and the global economic impact of IoT is projected to range between USD 2.7 trillion and 6.2 trillion by 2025 [3] [4].

II. Security of Iot Devices

As the Internet of Things technology has evolved over the past few years, the risks, and threats to which these types of devices are exposed have not been left behind, and likewise, cyber attacks have increased in both quantity and sophistication. Every day malicious actors develop more ways and employ increasingly complex techniques and tactics to compromise the security measures and to exploit vulnerabilities on Internet of Things devices. Cybersecurity and privacy have become one of the main issues for IoT devices and monitoring applications, and it's mainly because these devices contain plenty of information that attackers can use for their own benefit.

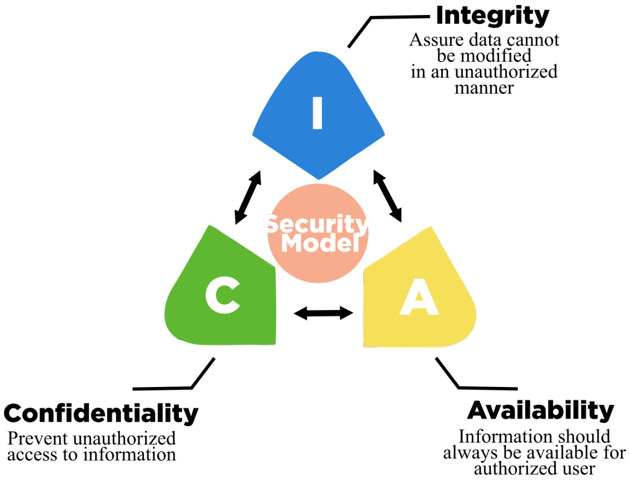
Integrity
Assure data cannot be modified in an unauthorized manner
I
Security Model
C
A
Confidentiality
Prevent unauthorized access to information
Availability
Information should always be available for authorized user

Fig. 1. CIA Triad

The statistic from these previous works provides us with a quantitative perspective to understand the scope and magnitude of the risks in security of IoT devices: According to [5], Over 85% of global organizations are projected to utilize IoT devices in various capacities, with around 90% of these businesses lacking confidence in the security of their IoT devices. Furthermore, approximately 70% of IoT devices are vulnerable to diverse attacks when connected to the internet, and a quarter of enterprise attacks are expected to result from compromised IoT devices. These statistics not only illustrate the magnitude of the security concern problems on IoT devices, but it also provides a solid foundation for further investigations and analysis.

To guarantee better security on IoT devices, it is imperative to always take into consideration the three key pillars of security, these pillars are known as the CIA, which are confidentiality, integrity, and availability as shown in Figure 1. Author [6] defines this pillars as follows: confidentiality as the protection of information against unauthorized access to ensure that only individuals or systems authorized have access to the information. Integrity refers to the authenticity of the data, meaning ensuring the integrity of data during communication or verifying the authenticity of information generated from the source. Finally, availability implies that authorized users should be able to access the data whenever they request it. Maintaining a focus on these three important pillars will help us to strengthen security and minimize the risk of vulnerabilities that are always present in this IoT devices.In order for the IoT system to ensure all of these three pillars it should be accompanied with different security methods or models. Security models should work as a whole to ensure these three pillars are always present on the IoT systems so that they can be reliable and secure. This three pillars represent an important role in safeguarding these interconnected devices they become indispensable to preserve the trustworthiness of IoT devices and applications. Since data is always being transferred between the device and the cloud it should always be protected, always available and ensure that no unauthorized users can have access to it.

III. Methodology

The main goal of this literature survey aims to investigate on the current mitigation strategies that are being employed in addressing the IoT devices attacks. This work's purpose is to gather insights into different approaches, tools and research carried out by different authors to secure the IoT systems. This work represents the derived findings by thoroughly exploring different IoT security- specific papers extending from 2019-2024, inclusively. The aim was to extract and summarize relevant, common, and impactful IoT security mitigation methods that are being used and inspire researchers for their future

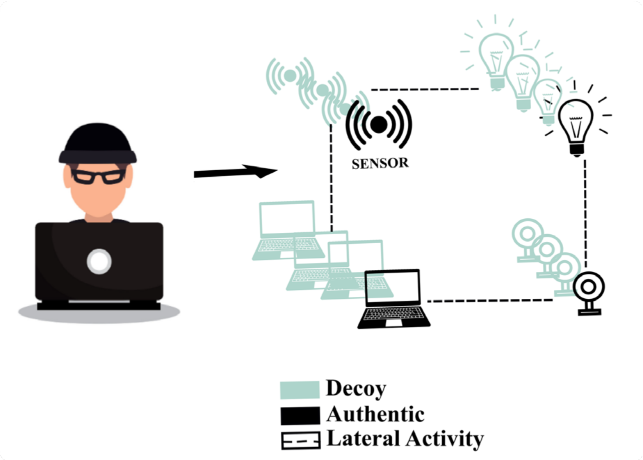

Fig. 2. Deception using Decoys

investigations on this field. This work categorizes the different methods and tactics that can be used to make the IoT systems and devices more reliable and enhance their security. The investigations cited on this work were selected research in which the author's contributions defined, analyzed, emulated, or simulated the mitigation method or model proposed to mitigate and detect different IoT security attacks.

IV. Using Deception for IoT Security

Deception, as the word says it, is to trick or mislead someone by creating false impressions, information or also to manipulate perceptions. In the past few years the cyberspace has adopted this term as cyber deception and author [7] describes it as intentional actions taken to deceive and/or confuse attackers, influencing them to either take or refrain from certain actions that support computer security defenses. Basically, how cyber deception function is a two-step action that includes the defender crafting information that is used to mislead the adversary and the adversary making wrong actions because of the deception.

D. Weissmen in his research proposes to use deception by the creation of duplicates of IoT devices using decoys. as a way to mitigate security risks by confusing the attack target. By having multiple of impostor devices exceeding the number of authentic operational working devices, the likelihood of attackers infecting and gaining control over the targeted IoT endpoint will be reduced [8]. This can be achieved using elements like software instances in virtual machines and it will also facilitate an easier management for network and security administrators. Figure 2 shows a graphic on how this model works by having different decoys for deception making it harder for the attacker to get to the targeted IoT device.

A framework for dynamic defense in SDN IoT-Edge Networks was suggested in [9] for cyber deception. The mechanism in this research produced a satisfactory outcome by supplying a protective measure to UDP, TCP SYN and LAND DDoS attacks by avoiding the compromise of IoT devices through temporary network addresses, without causing additional burdens and ensuring consistent system performance through proactive security measures. This framework is deceptive as it presents a misleading representation of the true network address, this approach acts defensively by preventing communication with the misrepresented hosts. Simultaneously, it consistently filters out unidentifiable traffic, clears flows, and alters IP mappings.

Another research on using deception for mitigating attacks on IoT devices was taken by [10]. In his work, a HoneyComb was proposed as a dark net-centric preemptive cybersecurity defense approach to mislead IoT devices compromised by malware and gather IoT forensic evidence of malware. They achieved this cyber defense method by utilizing IoT scans obtained from the dark net. They established an extensive dark net network as a substantial honeypot by constructing a honeycomb on the premises, enabling widespread interaction with malware-infected IoT devices. As a result, a broad perspective is obtained, and it can provide an extensive and robust examination of the cybersecurity stance when compared to the standard IoT honeypots which are much more restricted. A record of 1,432,518 interactions and 37,323 malware compromised IoT devices was obtained linked to over 40 types of IoT malware. As a result, a large vantage point of dark net IP addresses, one cloud-based IoT honeypot, and a cluster of virtualized IoT systems helped achieved deception.

V. Using REST APIs for IoT Security

As mentioned in this article, the development of alternative IoT monitoring cloud based applications is introducing new and evolving cyber risks to the protection and confidentiality. of the devices and the user's information. To the many risks that these devices are exposed to there is a need to implement IoT systems with robust security measures to prevent attackers from infiltrating the network through the IoT devices and to make sure data is secure while traveling from the device to the cloud. [11] research provides details on how the use of REST (Representational State Transfer) APIs enable the secure exposure of connected devices to both cloud-based applications and users.

This research proposes a model in which middleware is predominantly employed to make device data accessible through REST, concealing the intricacies and serving as a user interface for interacting with sensor data. This model can be used to prevent man-in-the-middle attacks because the API can undergo authentication with the server, and conversely, the server can authenticate with the API. Utilizing REST for machine-to-machine connectivity, IoT APIs enable the secure exposure of connected device data to users, that is why REST APIs are being used widely in the development of IoT networks. The data transfer in REST APIs is typically accomplished by JSON or XML over HTTP protocol, serving as an effective model for heterogeneous systems [12]. A middle ware platform can manage diverse models, acting as the intermediary between smart devices and cloud-based applications. Through the incorporation of a middle ware platform with abstract hardware, it can furnish APIs for communication, data processing, computation, privacy, and security.

As shown in Figure 3 this model shows the integration of API Models and REST APIs with a middleware between the communication of the device and the cloud application. Gateways facilitate the secure exchange of all information through the REST API. The middleware is responsible for managing device registration, identification, and database operations. It ensures data privacy and security by exposing stored data only after authentication and authorization through the REST API. This model proposed, while it doesn't guarantee a non-vulnerable IoT network, it for sure can help in the mitigation on man in the middle IoT attacks.

VI. Enhancing IoT security through the use of Blockchain.

Blockchain technology, also referred to as a distributed shared ledger, is an immutable database of records secured by cryptography. This type of technology enables the transfer and storage of digital assets without requiring third-party oversight. There is no requirement for a central authority because devices engage in direct asset exchange with each other, a process known as peer-to-peer. Thanks to these features blockchain can be a promising mitigation solution to manage many security attacks and issues on IoT devices inter networking and communication, Blockchain is a technology that can be well used to enhance the overall security features on IoT technology [13].

In a research carried out by [14] authors incorporated a blockchain in overall Internet of Things system to improve the security of the system indifferent parameters. One of the parameters was access control, with the incorporation of blockchain. Internet of Things devices are signed digitally preventing unauthorized entry. Secure storage was achieved due to the information on every transaction being kept in the blockchain, so the data's integrity can consistently be confirmed. Distributing IoT device

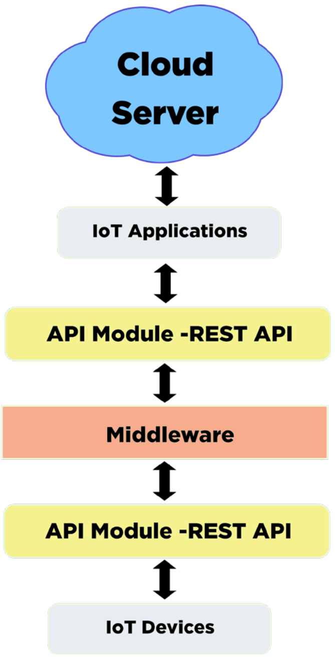

Fig. 3. An IoT system utilizes REST API and Middleware

firmware information via the blockchain platform ensures firmware authenticity, verifying the authenticity prior to booting and upgrades. This functionality aids in combating malware and counterfeiting. In the aspect of communication and secure status, each device undergoes authentication through a digital signature and utilizes a secure API for data communication, ensuring the overall system's security and integrity. The secure state using blockchain ensures that the smart device will stay secure state even if it fails or if it suffers from any kind of attack.

Leveraging blockchain technology in IoT systems greatly improves the overall security, transparency, and trustworthiness of the system. Additionally, it enhances reliability by incorporating features such as fault tolerance. Although it's known that introducing blockchain is not a simple or straightforward solution it certainly opens up space for more research and investigation on how to implement to mitigate several security attacks on IoT devices.

VII. Using Machine Learning in IoT Security

With the continuous advancement of IoT technology, an increasing amount of malware is being spread online and the proliferation of botnets has risen over the years. Malicious software initially establishes a botnet, spreading the bot across a network, and the botnet is utilized in situations involving a large number of infected computers. Numerous studies aim to discover methods for safeguarding the IoT environment from botnet attacks. Nevertheless, significant gaps persist in the development of an efficient detection mechanism [15].

A proposed model for mitigating this botnet attacks was carried out in [16] incorporates Machine Learning in Internet of things technology with cybersecurity. In this model, cybersecurity involved creating botnets and conducting diverse malware analyses by configuring attacker and client machines, and analyzing packets using Wireshark packet capturing tools. At the end, the machine learning models developed predict the analyzed packets. The study proposed certain contemporary machine learning approaches to recognize botnets and malicious traffic behavior. The author used decision tree, linear SVC, random forest, logistic regression, gradient-boosted decision tree and ensemble. Following the development of the model, the outcomes indicated that both the ensemble model and the gradientboosted decision tree model surpassed the performance of other classification models. This method can be utilized to identify various botnet attacks and other types of disruptive network activities. Another finding from this study indicated that a single dataset can serve as the foundation for training a majority of machine learning-based botnet detection models. Researchers could further extend this approach in future work by testing it with novel types of botnets and evaluating their performance and execution time. Utilizing diverse benchmark botnet datasets, a dynamic framework could be developed to predict future botnet behavior.

VIII. Other Threats and Solutions on IoT Security

IoT security encounters many risks and threats, and can be classified threats in different layers. Based on layers author [15] present the following threats and possible solution to prevent and mitigate different cybersecurity attacks and vulnerabilities. For the sensing layer on IoT systems, which is the lower layer in that architecture, security on hardware is the priority. For authentication on hardware, digital signatures can be applied alongside cryptographic hash algorithms that can aid in mitigating potential side-channel attacks. For data privacy on the sensing layer applying a lightweight cryptographic algorithm can prevent unauthorized access to the sensor data.

For the network layer, which has many different embedded wireless devices, communication and monitoring can accomplished at this layer, to achieve this, it must establish a strong authentication process employing a point-to-point encryption algorithm to thwart unauthorized access to the nodes. For security on routing IoT Systems mplementing multiple routing paths is crucial to guarantee the security of routing and the ability to detect errors. This layer, typically, is a vulnerable target for eavesdropping, unauthorized access, and Denial of Service (DoS) attacks. Attackers analyze eavesdropping and network congestion to exploit network privacy and confidentiality. The elevated likelihood of such attacks primarily stems from the distant access mechanism used for IoT and information exchange. To safeguard against any unauthorized access, the key exchange technique should be implemented with a high level of security [6].

For the middleware layer, which is in the middle of the network layer and the application layer, implementing an improved lightweight cryptography algorithm can guarantee confidentiality in both data exchange and storage. Another reliable solution that can be used is using decentralized blockchain for reliable and secure data protection instead of using centralized cloud services.

For the application layer, which is the one for the user, it should be the most secured layer, it should provide the user with multiple authentication services by providing the required hash value data for authentication. A firewall can also be used to enhance security. These are some of the possible solutions that can be researched on or test reliability to make IoT systems more secure every day.

Another method used for and mitigation of DDoS attacks on Internet of things Network was proposed by [18]. The method proposed consists of a unusual statistical pattern based algorithm for detection technique which is called ODIT, Online Discrepancy Test. This algorithm effectively addresses the attack while causing minimal disruption to the regular service and performance of the device, it scales well to large systems and It doesn't depend on assumed baselines and attack patterns; instead, it achieves a rapid and precise detection and mitigation approach for covert DDoS attacks. Authors also introduced a innovative intrusion detection ads well as a mitigation framework which employed as an online, scalable, and nonparametric algorithm for detecting anomalies, this method can be further investigated to de applied to IoT systems as a technique for mitigation DDoS attacks.

A groundbreaking security mechanism called LEDEM for MDA sent by wireless IoT to the IoT server was proposed and tested by [19]. This model consisted of a machine learning model with semi supervision for detection of attacks and two varied approaches to mitigate IoT-related risks. This method was tested and proven to impede denial of service attacks to the endpoint users even in the event of a wireless IoT attack on the IoT server. Combining new technologies such as machine learning algorithms with the internet of things can make a powerful tool for future research. This method can be studied and delved deeper by probing into different machine learning models to enhance the accuracy of attack detection. In addition to denial-of-service attacks, various security breaches in IoT can pose issues for users. Integrating technologies can result in a comprehensive security solution that addresses all breaches and potential future attacks.

The last mitigation method reviewed for this survey was a anomaly mitigation framework for Internet of Things systems with the use of fog computing proposed in [20]. They proposed a hybrid framework using the fog computing paradigm employed to address the insufficient resources in IoT networks.

This computational paradigm alleviates the computational overhead and related operational demands involved in mitigating anomalies from resource-constrained IoT devices. They tested this model by dividing the framework into two modules, one model was based on signature and the other model was an anomaly based IDS. Both modules used a database containing blacklisted IP addresses and employed an extreme gradient booster classifier. That enabled detection modules to capitalize on their capabilities. The results were that the signature-based model ensured 100% system's ability to accurately detect known attacks through their source, coupled with the anomaly-based detection's acceptable accuracy in identifying zero-day attacks, ensures safety and improves reliability in the IoT network, as proposed by the authors.

IV. Conclusions

There are many different attacks that can contribute to disruption of any of the three pillars necessary to ensure the IoT devices integrity and security. Some of these attacks include botnets, unauthorized access, denial of service, man in the middle, eavesdropping, and physical attacks. As the Internet of things technology evolves so does the attacks, so it is important to be aware of and investigate the different methods and techniques that can be used to approach this problem. This paper presented some of the actual methods discovered, implemented, proposed, and simulated by many authors that contributed to making the IoT systems more secure and reliable. Although all these methods mentioned in this work can help reduce the risk of attacks, IoT devices are never a hundred percent secure and there are always attackers trying to exploit any minimum vulnerability they can find. Through the developing of this work, it is expected to other authors and research to get motivated to continue investigating on this topic and apply or discover new methods for future implementations.

References

[1] A.G. Menjivar, "Mobile App Development for Wireless Monitoring and Configuration of Sensors using ESP8266," in 2022 IEEE Central America and Panama Student Conference (CONESCAPAN), San Salvador, El Salvador: IEEE, Oct. 2022, pp. 1–6. doi: 10.1109/CONESCAPAN56456.2022.9959569.

[2] "Development of a Pure Sine Wave Current Inverter with IoT Monitoring | IEEE Conference Publication | IEEE Xplore." Accessed: Jan. 23, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/9959240

[3] M. H. Alsharif, A. Jahid, A. H. Kelechi, and R. Kannadasan, "Green IoT: A Review and Future Research Directions," Symmetry, vol. 15, no. 3, Art. no. 3, Mar. 2023, doi: 10.3390/sym15030757

[4] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and Security: Challenges and Solutions," Appl. Sci., vol. 10, no. 12, Art. no. 12, Jan. 2020, doi: 10.3390/app10124102.

[5] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via SoftwareDefined Security," IEEE Internet Things J., vol. 7, no. 10, pp. 10250–10276, Oct. 2020, doi: 10.1109/JIOT.2020.2997651.

[6] T. Varshney, N. Sharma, I. Kaushik, and B. Bhushan, "Architectural Model of Security Threats theirCountermeasures in IoT," in 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India: IEEE, Oct. 2019, pp. 424–429. doi: 10.1109/ICCCIS48478.2019.8974544

[7] C. Wang and Z. Lu, "Cyber Deception: Overview and the Road Ahead," IEEE Secur. Priv., vol. 16, no. 2, pp. 80–85, Mar. 2018, doi: 10.1109/MSP.2018.1870866.

[8] D. Weissman, “IoT Security Using Deception – Measuring Improved Risk Posture,” in 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), Jun. 2020, pp. 1–2. doi: 10.1109/WFIoT48130.2020.9221223.

[9] H. Galadima, A. Seeam, and V. Ramsurrun, “Cyber Deception against DDoS attack using Moving Target Defence Framework in SDN IOT-EDGE Networks,” in 2022 3rd International Conference on Next Generation Computing Applications (NextComp), Oct. 2022, pp. 1–6. doi: 10.1109/NextComp55567.2022.9932172.

[10] M. S. Pour, J. Khoury, and E. Bou-Harb, “HoneyComb: A Darknet-Centric Proactive Deception Technique for Curating IoT Malware Forensic Artifacts,” in NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, Apr. 2022, pp. 1–9. doi: 10.1109/NOMS54207.2022.9789827.

[11] “Securing IoT Devices and SecurelyConnecting the Dots Using REST API and Middleware.pdf.”

[12] “Design of Restaurant Billing System (E Bill Resto) by Applying Synchronization of Data Billing in Branch Companies to Main Companies Based on Rest API | IEEE Conference Publication | IEEE Xplore.”

[13] K. Košťál, P. Helebrandt, M. Belluš, M. Ries, and I. Kotuliak, “Management and Monitoring of IoT Devices Using Blockchain,” Sensors, vol. 19, no. 4, Art. no. 4, Jan. 2019, doi: 10.3390/s19040856.

[14] “IoT Security Enhancement Using Blockchain | IEEE Conference Publication | IEEE Xplore.” Accessed: Jan. 28, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/9792693

[15] R. Patel, Cyber Security in Domain of IoT: A Review Threats and Security. 2020. doi: 10.13140/RG.2.2.20037.47841.

[16]] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, “Machine Learning-Based IoTBotnet Attack Detection with Sequential Architecture,” Sensors, vol. 20, no. 16, Art. no. 16, Jan. 2020, doi: 10.3390/s20164372.

[17] “IoT Botnet Creation and Detection using Machine Learning | IEEE Conference Publication | IEEE Xplore.” Accessed: Jan. 28, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10141717

[18] “Timely Detection and Mitigation of Stealthy DDoS Attacks Via IoT Networks | IEEE Journals Magazine|IEEE Xplore.” Accessed: Jan. 29, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9316792

[19] “Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture | IEEE Journals Magazine | IEEE Xplore.” Accessed: Jan. 29, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8993716

[20] M. A. Lawal, R. A. Shaikh, and S. R. Hassan, “An Anomaly Mitigation Framework for IoT Using Fog Computing,” Electronics, vol. 9, no. 10, Art. no. 10, Oct. 2020, doi: 10.3390/electronics9101565.