Analysis of IoT Vulnerabilities and Proposed Solution Approach for Secure Real-Time IoT Communication

Anteneh Girma
Department of CSIT
University of the District of Columbia
Washington, USA
anteneh.girma@udc.edu

Nurus Safa
Department of CSIT
University of the District of Columbia
Washington, USA
nurus.safa@udc.edu

Antione Searcy
Department of CSIT
University of the District of Columbia
Washington, USA
antione.searcy@udc.edu

***Abstract*—The growing reliance on real-time communication in Internet of Things (IoT) devices raises concerns about security vulnerabilities. Our research identifies vulnerabilities in prevalent IoT protocols that could enable attackers to disrupt communication, compromise data, or even seize control of devices. By analyzing various threats in a test environment, we found that insecure device configurations and weak authentication mechanisms were the primary culprits. We demonstrate the effectiveness of implementing robust authentication, end-to-end data encryption, and network segmentation in mitigating these vulnerabilities. Our findings emphasize the need for proactive security measures in developing and deploying real-time IoT communication systems.**

Keywords— Data Encryption in IoT, IoT Network Segmentation, Threat Simulation in IoT Security, IoT Connectivity Issues, IoT Device Configuration, Unsupervised Environments, Autonomous Systems, Cloud Computing, Critical Applications, Security Standards

I. INTRODUCTION

Internet of Things (IoT) is a rapidly growing and highly in-demand technology with billions of interconnected devices. These devices are increasingly being used in critical applications, such as industrial control systems, smart grids, and medical devices that can be easily paired with similar devices or technology and accessed remotely. Moreover, communication between IoT devices and the command control station often involves other connected routing devices, which can be controlled remotely by hackers. These vulnerabilities allow hackers to disrupt communication between devices, infringe on privacy, access information, and even gain control of the devices resulting in having serious consequences.

IoT devices, such as smartphones, smartwatches, and tablets, are becoming increasingly popular and are storing more and more sensitive data, such as contact information, health records, and financial data. To protect this data, it is important to be able to securely delete it when it is no longer needed. Deleting data from IoT devices is not as simple as it seems. Even after you delete data, it may still be possible to recover it using data recovery techniques. This is because deleting data from an IoT device typically only erases the mapping between the logical address of the data and its physical location on the device. The actual data may still be intact at its physical location. This poses a security risk, as malicious actors could potentially recover deleted data from lost or resold IoT devices [1].

Despite their widespread adoption, the security posture of IoT devices remains critically compromised due to resource limitations and inadequate security architectures. They may also be deployed in unsupervised environments, making them more vulnerable to attack. Notably, communication with cloud servers over the internet is a common characteristic of IoT device operation, further exacerbating their security vulnerabilities. This means that if an IoT device is compromised, attackers could gain access to sensitive data stored on the cloud server. Researchers are working on a variety of ways to improve the security of IoT devices. The development of dedicated security standards and protocols for IoT devices presents a promising approach to mitigating their inherent vulnerabilities. Another approach is to develop new security software that can be installed on IoT devices. Educating users about IoT security risks and promoting robust password protocols, regular software updates, and mindful data sharing behavior are essential for mitigating device vulnerabilities [2].

Thanks to the miniaturization of electronics hardware, IoT devices are everywhere in this century. In all aspects of air, sea and land transportation, power grids, various industries, and most importantly and obviously the defense industry is highly dependent on IoT devices. In short, national security depends on IoT. Among these are the newly emerging autonomous systems that attracted our attention. Countries around the world are investing in building UAV (Unmanned Aerial Vehicle) technology that will change the scenarios of today's delivery. Often, these UAVs operate in a group called swam; a swarm can have any number of vehicles in it. It could also include UGVs (Unmanned Ground Vehicles). To carry out their missions, these vehicles are required to collaborate in real time. This means a

continuous real time data exchange between the devices and often a ground station or a command station. What makes these IoT devices so useful also makes them vulnerable.

II. Related Works

The Internet of Things (IoT) has the potential to make our lives easier and more efficient, and to revolutionize many industries. For example, it can be used to create smart homes, smart cities, and smart factories. It can also be used to improve healthcare, transportation, and environmental monitoring. IoT devices are typically low-power, low-resource devices that collect and transmit data. They can be divided into two types: edge devices and gateway devices. Security is a challenge for IoT devices because they are heterogeneous, ubiquitous, and interconnected. This makes them vulnerable to a wide range of attacks [3].

Limited resources in IoT devices impede the realization of secure communication channels. One approach is to use collaborative security, where multiple devices pool their resources to implement security measures. Proxies offer a resource-efficient approach to bolstering security for constrained IoT devices. However, existing approaches are not sufficiently adaptive or comprehensive to address the heterogeneity and scale requirements of IoT. In that work, authors introduce a general-purpose framework for secure communications by resource constrained IoT devices and instances. Their framework employs notions of resource-aiding that accommodate a wide range of heterogeneities in IoT. Enhanced processing and communication of supporting devices, alongside accessible edge, and cloud-based support, fuel this research direction [5].

As the significance of data processing and intelligent decision-making increases, a support or middleware layer between the network and application layers gains prominence. This layer facilitates data processing, analysis, and decision-making before presenting information to the application layer of a conventional IoT design. Cloud computing has emerged as a popular choice for the underlying support layer in many IoT systems. Its scalability, flexibility, and cost-effectiveness make it a suitable platform for managing and processing large datasets generated by IoT devices. The perception layer has limited capabilities and common security methods like node authentication, weak encryption, and access control. There are concerns about privacy attacks and crimes targeting the perception layer, including taking control of nodes, using malicious code, and injecting data [18].

Challenges of Secret Sharing in Wireless IoT Networks

Secret sharing in wireless communication is difficult due to eavesdroppers. Two methods are available: information-theoretic and channel reciprocity-based. The information-theoretic approach is highly sensitive to the eavesdropper's capabilities, while the channel reciprocity-based approach is more robust and exploits the fact that Alice and Bob can measure the channel better than an eavesdropper. The process of secret key generation involves three steps: random bit generation, information reconciliation, and privacy amplification [4].

III. IoT Device Communication

The Internet of Things (IoT) involves a lot of devices and data [6]. Furthermore, the demand increases for more smart devices (i.e.) smart sensors, smart watches, phones), leaving the real time communication of these sophisticated devices at risk due to the constant communicating, devices sharing sensitive data from users to the cloud, in many instances without a secured connection for the data to be secured. A key component in the device communication protocols. The extensive data generated by IoT devices can be collected and analyzed at varying timeframes, including real-time and periodic intervals. While the sheer volume of data presents a growing challenge, the governance of this data, particularly its storage and access control mechanisms, poses an even more significant concern [8]. Another challenge in device communication is deciding which communication protocol is appropriate for your security model. For example, hypertext transport protocol (HTTP) is essentially the blueprint in terms of device communication for IoT related devices. However, HTTP is not a one size fits all model for all interconnected IoT devices, securely.

The security of any IoT device is paramount, the triad confidentiality, integrity, and availability of the data should be ensured from end to end, as the device number increases across these networks, which in turn as a result, will expose vulnerabilities to these systems. Different IoT communication types, including Device-to-Device (D2D), Device-to-Cloud (D2C), and Device-to-Gateway (D2G), require evaluation for their impact on security architecture [13]. To assess the best factor for IoT communication, understanding the complexity of the system, the network availability, and location of the infrastructure can hinder accessibility.

IV. Existing Security Vulnerabilities Within IoT Device Communication

Various threats can harm computer systems and networks. These include malware, denial-of-service attacks, man-in-the-middle attacks, SQL injection, and cross-site scripting. Each of these threats can have a significant impact on an organization, ranging from data theft and system damage to operational disruption. By understanding these threats and taking steps to mitigate them, organizations can protect themselves from cyberattacks [6].

To have an efficient IoT communication gateway, there are many security controls that need to be in place prior to these

IoT devices being able to communicate to the gateway. Thus, many compromises are due to the lack of IoT governance, and education of the users setting the boundaries for the IoT architecture. For example, access control is a widely known security control for ensuring the physical security of data centers, buildings etc. If there aren't physical controls in place to prevent unwanted access to the building, then that control is a failure. Like IoT devices, not all IoT architectures should allow all users to access their gateway, a preventative control would be to implement Least privilege access control to reduce and define specific roles for that system. Device Security, Network-Based Vulnerabilities, and Software-Based Vulnerabilities represent the major attack vectors for IoT devices. Protecting against them requires a multi-layered approach focusing on secure hardware, robust network configurations, and up-to-date software with strong authentication and encryption [14].

DDoS Mitigation Strategies for Cloud-Based Services

Denial-of-Service (DoS) attacks aim to disrupt a network's ability to serve legitimate users, typically by flooding it with traffic or exploiting weaknesses in applications, protocols, or network devices. Distributed Denial-of-Service (DDoS) attacks amplify this effect by coordinating attacks from multiple systems. These attacks can be categorized based on their target (network bandwidth, connectivity, specific protocols, or network devices) and the methods used (exploiting bugs, sending invalid requests, or saturating resources) [21]. While cloud computing offers convenient remote access, its security vulnerabilities, including DDoS attacks and third-party data access, pose major risks. Existing DDoS mitigation techniques struggle against increasingly sophisticated attacks, prompting exploration of data mining techniques like Density-based spatial clustering of application with noise (DBSCAN) clustering to identify and combat these threats. Despite limitations, DBSCAN's effectiveness in handling diverse data clusters makes it a promising avenue for securing cloud services [22]. DDoS attacks pose a major threat to Cloud Service Providers (CSPs), potentially causing customer churn, legal headaches, and financial losses. These attacks come in various forms, targeting either cloud resources (e.g., DNS flood) or network bandwidth (e.g., UDP flood) using diverse tools like Agobot and Trinoo. To mitigate these risks, CSPs need to employ all available prevention and mitigation strategies. Remember, a disrupted cloud is a vulnerable cloud [23].

V. Advantages and Disadvantages of Existing IoT Security Solutions

Existing IoT security solutions have several advantages and disadvantages. The protocols in the paper of Naoui et al. satisfy the forward secrecy and key independence requirements, which are essential for protecting against many common types of attacks. Some of the protocols also have low bandwidth and key storage overhead, which is important for constrained IoT devices, and some are robust to message loss and fake messages, which is important for IoT networks that are prone to these types of errors. On the other hand, some of the protocols have relatively high computational overhead, which may be too much for some IoT devices. Some are also not robust to the 1-affect-n phenomenon, where the compromise of a single node can lead to the compromise of all nodes in the network. And some are centralized, which makes them susceptible to single points of failure [9].

TABLE I. ADVANTAGES AND DISADVANTAGES OF EXISTING IOT SECURITY SOLUTIONS

Solutions	Advantages	Disadvantages	Security Gap	References
Artificial Intelligence (as a security tool)	The explosive growth of AI-powered IoT devices marks a major turning point in computing, fundamentally reshaping the landscape with its vast interconnectedness and intelligence.	Fast-growing AI integration in homes risks leaving idle devices vulnerable due to insufficient management tools.	The surge of AI-powered IoT devices demands a paradigm shift in security. Every facet of data handling, from collection in individual devices to routing and analysis in the cloud, needs robust safeguarding.	10, 11
Machine Learning	Reporting existing vulnerabilities on real-time, Big IoT Data Analytics, Cyber Attack Detection, and Containment Delivering Threat Alert.	Malicious actors can use AI/ML to test and refine their malware, making it adept at breaching AI/ML-defended systems. This iterative learning risks escalating cyberattacks to catastrophic levels.	AI's effectiveness rests solely on the quality and accessibility of its training data. Without highly accurate datasets, it stumbles, lacking the inherent creativity or self-improvement capabilities of humans.	10, 12
IoT Service platform	Tailored IoT automation and rich data	Weaknesses in IoT network	The growing sea of IoT	19, 20

(customized)	empower manufacturers to boost efficiency and innovate solutions, and the designers to create more useful products.	security, increased bandwidth for increasing IoT devices. Additionally, increased monitoring time will be needed for devices.	devices generates a tidal wave of data, constantly flowing through interconnected networks. While this opens doors to efficiency and innovation, it also creates a vast attack surface for cyber threats. To ensure the safe and secure operation of these systems, a robust security strategy is crucial, encompassing both network and data protection measures.	

VI. Analysis of Existing Security Factors Affecting IoT Communication

Unlike traditional computers, many IoT devices lack native security measures, transmitting information unencrypted due to cost constraints and limited processing power. Manufacturers are attempting secure boot, network traffic encryption, and Secure Shell (SSL) implementations, but success hinges on proper execution to avoid vulnerabilities [8]. The burgeoning realm of the Internet of Things (IoT) carries immense promise for convenience and interconnectedness, yet simultaneously casts a long shadow of security concerns. From the Mirai and Bashlite botnet attacks to the evolving landscape of vulnerabilities, this burgeoning technology exposes a vast attack surface ripe for exploitation. While early attempts categorized threats based on the traditional three-layered architecture, the complex and diverse nature of modern IoT systems demands a more holistic and dynamic approach. As security threats transcend distinct layers and morph with rapid technological advancements, robust research and collaborative efforts across government, industry, and academia are paramount to unlocking the full potential of IoT while effectively mitigating the lurking security shadow [7].

The 2019 URGENT/11 vulnerabilities serve as a stark reminder of the cyberthreats looming over medical devices and hospital networks. These 11 flaws, including critical RCEs and DoS vulnerabilities, could grant remote attackers control of devices or disrupt their vital functions. This risk is compounded by findings like Trend Micro's 2018 study, highlighting exposed devices and supply chain weaknesses in connected hospitals. Securing this critical infrastructure demands a multi-pronged approach. Manufacturers must prioritize secure device design and collaborate with agencies like the FDA and DHS to standardize security practices. NIST's emphasis on SCRM further underscores the importance of safeguarding the entire supply chain. Healthcare facilities must hold third-party vendors to the same high security standards, while users have the responsibility to maintain device security and remain vigilant for signs of compromise. Only through the collective effort of all stakeholders can we mitigate the URGENT/11 threat and ensure the integrity of healthcare systems in the face of evolving cyberattacks [17].

IoT devices need to be connected to the Internet to communicate with each other. Communication between the three layers of the IoT can be done through wired or wireless connections, using heterogeneous communication technologies such as Ethernet, Wi-Fi, Bluetooth, and ZigBee. However, this heterogeneity makes it very difficult to manage and control IoT networks and applications. Additionally, the traditional three-layer architecture of IoT exposes weak controllability in the underlying wireless sensor network (WSN) and heterogeneity in the core network of the middle layer and the short-distance communication network [7].

VII. Proposed Solution Approach

Setting up the test environment involves using a desktop or laptop computer as the command station, a router, and four Raspberry Pi 4s as the IoT devices. The command station has no user account or administrative access, and the test environment is connected to a dedicated source of internet access that is isolated from the rest of the systems. Testing the setup for vulnerabilities is done by injecting various simulated threats into the hardware and software of the setup. Once the simulated threats have been injected, our team identifies the vulnerabilities that the threats were able to exploit. Once the vulnerabilities have been identified, we develop methods to mitigate them. This may involve installing security patches, changing configurations, or implementing new security measures. The test environment is monitored throughout the testing process to identify any unexpected behavior. The whole approach can be visualized with the following timeline of steps.

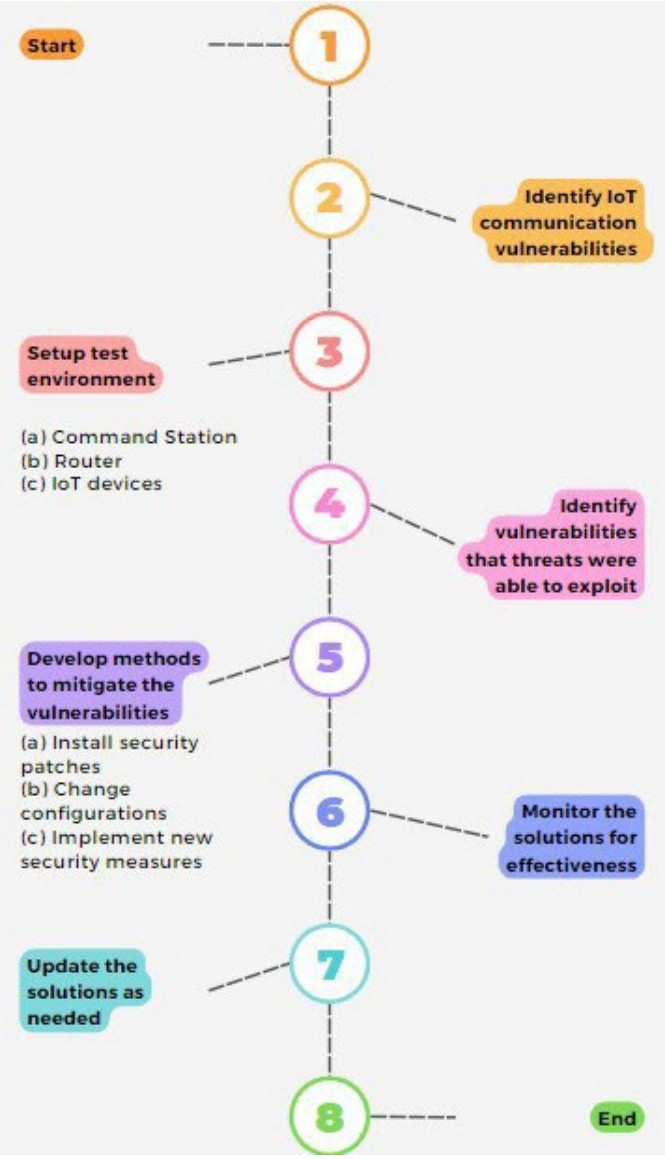

FIGURE I. TIMELINE OF PROPOSED SOLUTION APPROACH STEPS

A. Security Patches and Their Importance

Security patches are crucial for protecting software and devices from evolving cyber threats. They fix vulnerabilities that could allow attackers to steal sensitive information, hijack devices, or disrupt operations. While tech companies often release regular updates with patches included, sometimes critical vulnerabilities necessitate rapid releases, like Apple's recent patch to address high-risk flaws. Regardless of delivery method, promptly applying all security patches is essential for maintaining robust cybersecurity. Remember, even a single unpatched vulnerability can be the chink in your armor that attackers exploit [15]. The following are some of the best practices for Security Patches [15]:

- Security patches can be automatic or manual.
- Automatic patches are ideal, but you may need to configure your device or software to allow them.
- Manual patches require you to download and install the software files yourself.
- Only download security patches from trusted vendor websites and trusted network locations.

B. Implementation of New Security Measures

In the wake of heightened cyber threats and evolving attack vectors, the need for robust security measures has never been greater. To bolster defenses and mitigate risk, the implementation of innovative techniques is paramount. The following figure explores three such techniques.

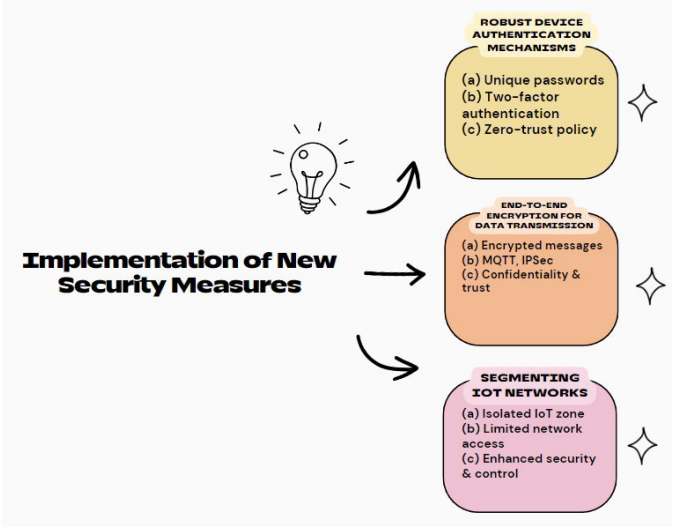

FIGURE II. IMPLEMENTATION OF NEW SECURITY MEASURES [16]

In today's omnipresent network landscape, the burgeoning realm of the Internet of Things (IoT) presents both transformative possibilities and lurking threats. Securing these interconnected environments necessitates a proactive and multifaceted approach, weaving a tapestry of defense across device access, data transmission, and network architecture. By diligently implementing robust authentication protocols, prioritizing end-to-end data encryption, and establishing secure network segmentation, we can transform these digitally augmented spaces from vulnerable frontiers into impregnable fortresses of privacy and security. Let's delve deeper into these defensive pillars, unveiling the strategies to craft a secure haven in the age of ubiquitous connectivity.

VIII. CONCLUSION AND FUTURE WORK

The increasing prevalence of IoT devices in critical applications has raised concerns about the security of IoT communication. Hackers can exploit vulnerabilities in IoT

communication to disrupt communication, infringe on privacy, access information, and even gain control of devices, resulting in serious consequences. This research project analyzes existing IoT communication vulnerabilities and proposes a solution approach to address these security issues. The proposed approach includes installing security patches, changing configurations, and implementing new security measures to protect IoT communication from cyberattacks. It provides a systematic and comprehensive method for identifying and mitigating IoT communication vulnerabilities. The test environment setup allows for a controlled and isolated environment to test for vulnerabilities and develop mitigation strategies. The approach is based on identifying vulnerabilities through simulated threats and then developing methods to mitigate those vulnerabilities. The test environment is monitored throughout the process to identify any unexpected behavior. Despite its promising potential, the proposed solution approach exhibits limitations in scope, reliance on testing, risk of false positives, and limited generalizability. These limitations, while not insurmountable, warrant further investigation and refinement. Future research could focus on expanding the scope, mitigating false positives, and exploring alternative implementation strategies for broader applicability. Additionally, continuous monitoring may be necessary to ensure long-term effectiveness.

The current approach relies on testing to identify vulnerabilities. This means that it may not be able to identify all vulnerabilities, especially those that are not obvious or that require specific conditions to be triggered. Future research could focus on developing more comprehensive methods for identifying vulnerabilities, such as using formal verification techniques or machine learning. The current approach is a standalone process that is not integrated with existing security processes. This can make it difficult to implement and maintain. Future research could focus on developing frameworks for integrating IoT communication vulnerability management into existing security processes, such as by using security information and event management (SIEM) systems or threat intelligence platforms.

ACKNOWLEDGEMENT

This research project is funded by NSF grant award# 2011689.

REFERENCES

[1] J. Xiong et al., “A Secure Data Deletion Scheme for IoT Devices Through Key Derivation Encryption and Data Analysis,” Future Generation Computer Systems, Volume 111, October 2020, Pages 741-753.

[2] S. Amanlou, M. K. Hasan, and K. A. Abu Bakar, “Lightweight and Secure Authentication Scheme for IoT Network Based on Publish–Subscribe Fog Computing Model,” Computer Networks, Volume 199, 9 November 2021, 108465.

[3] L. F. Khalid and S. Y. Ameen, “Secure IoT integration in Daily lives: A Review,” Journal of Information Technology and Informatics, Vol. 01, No. 01, pp. 6-12(2021).

[4] W. Xi et al., “Keep: Secure and Efficient Communication for Distributed IoT Devices,” IEEE, 23 July 2020.

[5] A. M. Taha, A. M. Rashwan, and H. S. Hassanein, “Secure Communications for Resource-Constrained IoT Devices,” MDPI, 29 June 2020.

[6] I. Ahmad, R. A. Ziar, and M. S. Niazy, “Survey on IoT: Security Threats and Applications,” Journal of Robotics and Control (JRC), Volume 2, Issue 1, January 2021.

[7] J. Zhang, H. Chen, L. Gyong, J. Cao, and Z. Gu, “The Current Research of IoT Security,” IEEE, June 2019.

[8] S. Narang, T. Nalwa, T. Choudhury and N. Kashyap, "An efficient method for security measurement in internet of things," 2018 International Conference on Communication, Computing and Internet of Things (IC3IoT), February 2018.

[9] S. Naoui, M. E. Elhdhili and L. A. Saidane, "Security analysis of existing IoT key management protocols," 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016.

[10] T. G. Zewdie and A. Girma, “IoT Security and The Role of AI/ML to Combat Emerging Cyber Threats in Cloud Computing Environment,” Information Systems Journal 21(4):253-263, November 2020.

[11] P. Efstathopoulos, “Cloud Security Is Overwhelming. AI and Machine Learning Can Help,” Symantec Enterprise Blogs, 29 July 2019.

[12] “Cloud Computing & IOT,” esds, 7 July 2021.

[13] V. Rudyi, “Overview of IoT Device Communication,” AgileVision, July 2023.

[14] P. Malhotra et al., “Internet of Things: Evolution, Concerns and Security Challenges,” MDPI, 5 March 2021.

[15] E. Heaslip, “What Are Security Patches and Why Are They Important for Your Business?,” U.S. Chamber of Commerce, July 2023.

[16] V. Padua, “IoT Security: Safeguarding Critical Networks Against Digital Assaults,” Cybersecurity Exchange, September 2023.

[17] “FDA warns against urgent/11 vulnerabilities affecting medical devices and Hospital Networks,” Nouvelles de Sécurité - Trend Micro FR, October 2019.

[18] T. Mazhar et al., “Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence,” brain sciences, April 2023.

[19] H. Taherdoost, "Security and Internet of Things: Benefits, Challenges, and Future Perspectives," Electronics, vol. 12, no. 8, p. 1901, Apr. 2023, doi: 10.3390/electronics12081901.

[20] B. Flavin, “Internet of Things: Weighing the Pros and Cons,” Rasmussen University, 2022.

[21] T. G. Zewdie and A. Girma, "AN EVALUATION FRAMEWORK FOR MACHINE LEARNING METHODS IN DETECTION OF DOS AND DDOS INTRUSION," 2022 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), 2022, pp. 115-121, doi: 10.1109/ICAIIC54071.2022.9722661.

[22] Girma A., Wang P., (2018) AN EFFICIENT HYBRID MODEL FOR DETECTING DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS IN CLOUD COMPUTING USING MULTIVARIATE CORRELATION AND DATA MINING CLUSTERING TECHNIQUES, IACIS Journal, Issues in Information Systems, Volume 19, Issue 2, pp. 1-12, 2018.

[23] Anteneh Girma, Moses Garuba, Jiang Li, Chumei Lui, Kobi Abayomi “ANALYSIS OF DDOS ATTACKS AND AN INTRODUCTION OF A HYBRID STATISTICAL MODEL TO DETECT DDOS ATTACKS ON CLOUD COMPUTING ENVIRONMENT”, ITNG 2016.