©NIJEP
Publications

Open Access
Online ISSN: 2992-5487
Print ISSN: 2992-6068

NEWPORT INTERNATIONAL JOURNAL OF ENGINEERING AND PHYSICAL SCIENCES (NIJEP)

Volume 4 Issue 1 2024

https://doi.org/10.59298/NIJEP/2024/411722.1.1100

Enhancing Security in Internet of Things (IoT) Architecture through Defense-in-Depth Mechanism: A Comprehensive Study

[1]Chika Lilian Onyagu, [2]Okonkwo Obikwelu, [3]Akawuku Godspower and [4]Joshua John
[1]Department of Cybersecurity, Faculty of Computing and Information Technology, Margaret Lawrence University, Umunede Delta state, Nigeria
[2,3]Department of Computer Science, Faculty of Physical Sciences, Nnamdi Azikiwe University, Awka, Nigeria.
[4]Institute of Computing & ICT, Ahmadu Bello University, Zaria, Nigeria

ABSTRACT

The Internet of Things (IoT) has revolutionized various domains, offering connectivity and data sharing among diverse devices and services. However, this interconnectedness poses significant security challenges, primarily centered around confidentiality, integrity, and availability. This paper investigates the security issues embedded in the layers of IoT architecture, ranging from the perception layer to the application layer. By leveraging the Defense-in-Depth security mechanism, we propose a comprehensive approach to fortify IoT systems against cyber threats. The Defense-in-Depth strategy is illustrated through a layered model, addressing security concerns at the perimeter, host, OS/application, and data layers. The study explores various security measures applicable to each layer, emphasizing the need for a multi-faceted approach to ensure the robustness of IoT security.

Keywords: Internet of Things (IoT), Security Issues, Defense-in-Depth Mechanism, Perception Layer, Network Layer, Data Processing Layer, Application Layer, Confidentiality, Integrity, Availability

INTRODUCTION

Internet of things (IoT) is a collection of interconnected objects, services, people, and devices that can communicate, share data, and information to achieve common goals in different areas and applications. The purpose of IoT is to transform the way we live today by enabling intelligent devices around us to perform daily tasks and chores with minimal human intervention [1-4]. IoT can be implemented in many different domains including transportation, agriculture, healthcare, wearable, connected vehicles and transport and others. The major challenges in IoT application is the security threats associated with these devices and advancement of cyber-attacks. The security issues of IoTs violates the security Triad: Confidentiality, Integrity and Availability. The violation of these threats can be at any layer of IoT architecture [5-7]. In order to understand the security issues associated with Internet of Things, this paper studied the architecture of IoTs and possible security attacks on them. IoT reference architecture serves as a foundational blueprint that outlines the essential components and interactions within an IoT system [8-9]. It provides a solid starting point for designing and implementing IoT solutions. IoT reference architectures typically consist of multiple layers that work together to enable the functioning of an IoT system. [1], explain the four layers of IoT Architecture which includes; Perception, Network, Processing layer and the Application layer.

Perception Layer: This layer comprises the physical devices or sensors that collect data from the environment or interact with the physical world. These include temperature sensors, motion detectors, cameras [10].

Network Layer: The network layer facilitates the connectivity and communication between the IoT devices and the cloud. It includes protocols, gateways, routers, and other networking infrastructure to ensure seamless data transfer and reliable connections [11].

Data Processing Layer: This layer involves processing and analyzing the data collected from IoT devices.

Application Layer: The application layer encompasses the software applications or services that utilize the processed IoT data to provide specific functionalities or address specific use cases [12].

Example: real–time monitoring and control systems to predictive analytics, machine learning algorithms, and automation. The purpose of this paper is to present the security issues associated with IoTs and better approach to

Open Access
Online ISSN: 2992-5487
Print ISSN: 2992-6068

manage these issues using Defense-in-depth security Mechanism. The security mechanism focus on managing the issues with multiple approaches to reduce surface attack on devices [13].

METHODS

The research methodology involves an in-depth analysis of the existing literature on IoT security issues and Defense-in-Depth strategies. The IoT architecture is dissected, focusing on the four layers: Perception/Physical, Network, Data Processing, and Application. Relevant security threats at each layer are identified and correlated with specific Defense-in-Depth measures. The proposed security measures are structured based on the layers and aligned with the established Defense-in-Depth model.

RELATED WORK

The rapid proliferation of the Internet of Things (IoT) has ushered in a new era of connectivity, transforming the way we live, work, and interact with the world. However, this technological revolution brings with it a host of security challenges that demand attention. This essay delves into the extensive body of literature surrounding IoT security issues, shedding light on the multifaceted nature of these challenges and the measures proposed to mitigate them. .The heterogeneity of the IoT is the first challenge it has encountered, as each of these various systems or devices uses circuitry and protocols that are distinct from the others [2]. [3], explained that the diverse nature of IoT devices and technologies makes achieving a standardized security framework challenging, and addressing these challenges requires a holistic approach.

[4], work on the vulnerability of IoT devices highlight issues like insecure hardware, weak authentication, and the lack of encryption in IoT devices. These vulnerabilities expose devices to potential exploitation, leading to unauthorized access, data breaches, and compromise of device integrity.

[5], underscore the importance of addressing inadequate data encryption, insufficient access controls, and the prevalence of man-in-the-middle attacks. The interconnected nature of IoT devices demands robust network security measures to safeguard against unauthorized access and data interception. [6], research on IoT Cloud security discuss issues like insecure APIs, data breaches, and unauthorized access to cloud resources. [7], explained on importance of Cloud IoT security, the explained that the integrity and confidentiality of data stored in the cloud become paramount, necessitating measures such as secure cloud configurations, encryption, and continuous monitoring [7].

[8], predicted that there would be 6.58 billion people and 50 billion IoT devices on the earth by 2020. Evans' estimate of 50 billion IoT devices by 2020 was not the only one; the DHS Cybersecurity Strategy predicted that by 2020 there would be 20 billion networked devices connected to the cyber domain. (DHS Cybersecurity Strategy | Homeland Security, n.d.) IoT Security Solution using Defense-in-Depth

SECURITY ISSUES ON IOT LAYER ARCHITECTURE

I. Perception/Physical: While this layer plays a crucial role in enabling IoT functionality, it also presents specific security challenges. Here are some security issues on the physical layer:

Node Tempering: Issue: IoT devices in the perception layer are often deployed in diverse and uncontrolled environments, making them susceptible to physical attacks and tampering [8].

Data Integrity and Accuracy: Sensors in the perception layer generate data that is crucial for decision-making in the entire IoT system. Malicious actors may compromise the data generated by sensors, (malicious code injection) leading to inaccurate information and potentially affecting downstream processes.

Unauthorized Access to Sensors: Unauthorized access to sensors in the perception layer can result in data interception, manipulation, or denial of service [9].

II. Network Layer security issues

The network layer of IoT is susceptible to the following attack:

Denial-of-Service (DoS) Attacks: IoT networks are vulnerable to DoS attacks, which can overwhelm the network infrastructure and disrupt normal operations. Service interruptions, delayed data transmission, and potential damage to IoT devices [9].

Man-in-the-Middle (MitM) Attacks: MitM attacks involve intercepting and altering communication between IoT devices, compromising data integrity.

Unauthorized access to sensitive information, manipulation of data, and potential injection of malicious commands.

II. Data Processing layer: the processing layer is vulnerable to various security issues. Here are some common security challenges associated with the layer of IoT architecture:

Data Integrity: Unauthorized access or tampering of data within the processing layer can compromise the integrity of the information [5].

Denial of Service (DoS) Attacks: The processing layer may be vulnerable to DoS attacks, where an attacker overwhelms the system with excessive requests, causing a disruption in data processing [7].

Insufficient Authentication and Authorization: Weak authentication mechanisms or inadequate authorization controls may allow unauthorized entities to gain access to sensitive data within the processing layer [7].

Open Access
Online ISSN: 2992-5487
Print ISSN: 2992-6068

Insecure APIs (Application Programming Interfaces): attackers to gain unauthorized access or inject malicious data can exploit Insecure APIs within the processing layer [6].

III. The application layer of IoT: the architecture is crucial for enabling communication and interaction between IoT devices and end-users or other applications. However, this layer is also susceptible to various security issues as follows:

Insecure Application Programming Interfaces (APIs): APIs play a crucial role in facilitating communication between IoT devices and applications. Insecure APIs can expose sensitive data and functionalities, leading to unauthorized access [6].

Lack of Secure Authentication and Authorization: Weak or nonexistent authentication mechanisms can lead to unauthorized access, allowing malicious actors to manipulate or control IoT devices [10].

SECURITY GOALS OF IOT

Traditional security goals are generally known as the "Confidentiality, Integrity, and Availability triad (CIA-triad). The purpose of every organization is to ensure that:

Confidentiality: Confidentiality is one of the fundamental goals in IoT (Internet of Things) security, and it refers to the protection of sensitive information from unauthorized access, disclosure, or exposure. In the context of IoT, confidentiality is crucial because IoT devices often handle sensitive data, such as personal information, health records, or proprietary business data. Organizations can enhance the confidentiality of data in IoT environments, reducing the risk of unauthorized access and data breaches. It's important to note that a comprehensive security strategy should involve a combination of technical measures, policies, and ongoing monitoring to adapt to evolving threats in the IoT landscape.

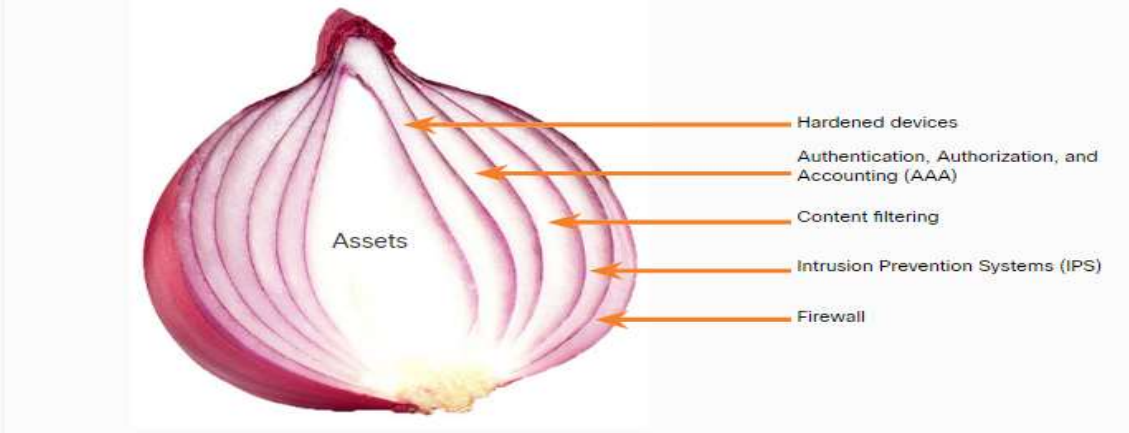
Availability: Availability is a critical goal in IoT (Internet of Things) security, ensuring that IoT systems and devices are accessible and operational when needed. This goal involves preventing and mitigating disruptions, downtime, or attacks that could compromise the functionality and accessibility of IoT services. Organizations can enhance the availability of IoT systems, ensuring that they remain accessible and operational even in the face of potential disruptions or security incidents. Availability, alongside confidentiality and integrity, forms a crucial component of a comprehensive IoT security strategy.

Integrity: Integrity, as a security goal in the context of the Internet of Things (IoT), refers to the assurance that data remains accurate, unaltered, and trustworthy throughout its lifecycle. Ensuring the integrity of IoT systems is essential to prevent unauthorized or malicious manipulation of data, which could lead to false information, incorrect decisions, or compromised functionality. Organizations can enhance the integrity of IoT systems, ensuring that data remains reliable and unaltered. Integrity, along with confidentiality and availability, forms a triad of essential security goals for comprehensive IoT security.

SECURING IOT ARCHITECTURE USING DEFENSE-IN-DEPTH MECHANISM

Defense in depth is a strategy that leverages multiple security measures to protect an organization's assets. The purpose of the defense is that if one layer is compromised, additional layers exist as a backup. Defense in depth addresses the security vulnerabilities inherent with not only hardware and software but with people, as negligence or human error are often the cause of a security breach. Today's cyber threats are growing rapidly in scale and sophistication [8]. Defense in depth is a comprehensive approach that employs a combination of advanced security tools to protect an organization's endpoints, data, applications, and networks. The goal is to stop cyber threats before they happen, but a solid defense-in-depth strategy also thwarts an attack that is already underway, preventing additional damage from taking place [9]. The defense-in-depth strategy concentrates on not only the security weaknesses of hardware and software, but it also focuses on negligence or human error that are often the cause of security breaches. A common analogy used to describe a defense-in-depth approach is called "the security onion." As illustrated in figure

Open Access
Online ISSN: 2992-5487
Print ISSN: 2992-6068



Security Onion [9]

Defense-in-depth security model has four layers [10 -13];

Layer 1 (Perimeter Defense): this dense mechanism focus on securing the network and its connected devices. In IoT architecture, this mechanism will protect the physical devices and its network.

Layer 2(Host protection): the host here referred to all other systems connected to the network. The IoT Application and Data processing layer falls to this category. By using Strong IDPS (Intrusion detection and Prevention systems) and firewall manages security at this layer.

Layer 3(OS/Application security): this layer protects the operating system and the Applications

Layer 4 (Data /Information Protection): this layer focus on protecting Data and Information by implementing appropriate measures to ensure Data integrity.

Open Access
Online ISSN: 2992-5487
Print ISSN: 2992-6068

Table 1: Application of security measures on IoT layers

S/N	IoT Layer Layer	Security issues	Measures
1.	Perception/Physical	i. Node Tempering: ii.Unauthorized Access to Sensors iii. Data Integrity and Accuracy	Implementing physical security such as tamper-evident packaging, CCTV etc. strong authentication mechanisms & secure access controls. Implementing secure communication protocols, data validation mechanisms, and cryptographic techniques.
2.	Network Layer	I. Denial-of-Service (DoS) Attacks ii. Man-in-the-Middle (MitM) Attacks	Employ traffic filtering, rate limiting, and anomaly detection mechanisms to mitigate them. Implement secure communication protocols, use digital certificates, and regularly update cryptographic algorithms.
3.	Data Processing layer	i.Data Integrity attack iii. Denial-of-Service (DoS) Attacks iii. Insufficient Authentication and Authorization:	Implement robust encryption and access controls to ensure data integrity Employ traffic filtering, rate limiting, and anomaly detection mechanisms to mitigate them. Enforce strong authentication protocols and granular authorization mechanisms to restrict access only to authorized users and devices.
4.	Application layer	ii. Insecure API iii. Lack of Secure Authentication and Authorization	Implement secure coding practices for APIs, use authentication and authorization mechanisms, Implement strong authentication methods such as multi-factor authentication, and enforce proper authorization controls to restrict access

[7-9]

CONCLUSION

Various research had shown that the application of IoT and its benefit in a various human life activities cannot be over-emphasized. To fully benefit from IoT technology across all devices for communication purposes, it is essential to prioritize solid strategies for securing these endpoints. Scholars underscore the need for a multifaceted approach, encapsulated by the Defense-in-Depth mechanism, to address the myriad security concerns. As technology continues to advance, ongoing research and collaborative efforts are essential to stay ahead of

Open Access
Online ISSN: 2992-5487
Print ISSN: 2992-6068

emerging threats and ensure the security and integrity of our increasingly interconnected world. For further, studies, the research recommend more advanced security measures in managing IoT security problems.

REFERENCES

1. Leo,M., Battisti,F., Carli,M., and Neri,A.,(2014). "A federated architecture approach for Internet of Things security," in Euro Med Telco Conference (EMTC),
2. Butun, I., Osterberg, P., & Song, H. (2020). Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. IEEE Communications Surveys & Tutorials, 22(1), 616–644. https://doi.org/10.1109/comst.2019.2953364
3. Abomhara,M., and Koien, G.(2014)."Security and privacy in the Internet of Things: Current status and open issues," in Int'l Conference on Privacy and Security in Mobile Systems (PRISMS).
4. Gazis, A. (2021). What is IoT? The Internet of Things explained. Academia Letters. https://doi.org/10.20935/al1003
5. Gupta,S., and Gupta,B.(2017) Cross-Site Scripting (XSS) attacks and defense mechanisms: Classification and state-of-the-art. *Int. J. Syst. Assur. Eng. Manag.* ;**8**:512–530. doi: 10.1007/s13198-015-0376-0.
6. Wiley,S., and Park,O.(2011). "Pin-hole firewall for communicating data packets on a packet network
7. Alaba and Ayotunde, (2017). "Internet of things Security: A Survey." Journal of Network and Computer Applications.
8. Evans, D. (2011). The Internet of Things how the next evolution of the internet Is changing everything. Cisco Internet Business Solutions Group (IBSG). https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
9. Prabhakar, S.(2017) Network Security in Digitalization: Attacks and Defence. *Int. J. Res. Comput. Appl. Robot.*
10. Bharathi, M., Tanguturi, R., Jayakumar, C.,& Selvamani. K.(2012) Node capture attack in Wireless Sensor Network: A survey; Proceedings of IEEE International Conference on Computational Intelligence & Computing Research (ICCIC); Coimbatore, India.
11. Lee,Y., Lin, and Huang,H.,(2014) "A lightweight authentication protocol for internet of things," in Int'l Symposium on Next-Generation Electronics (ISNE
12. Sicari, and Sabrina, (2015)."Security, privacy and trust in Internet of Things: The road ahead." Computer Networks
13. Misra and Gourav, (2016)."Internet of things (IoT)–a technological analysis and survey on vision, concepts, challenges, innovation directions, technologies, and applications" American Journal of Electrical and Electronic Engineering.

CITE AS: Chika Lilian Onyagu, Okonkwo Obikwelu, Akawuku Godspower and Joshua John (2024). Enhancing Security in Internet of Things (IoT) Architecture through Defense-in-Depth Mechanism: A Comprehensive Study .NEWPORT INTERNATIONAL JOURNAL OF ENGINEERING AND PHYSICAL SCIENCES, 4(1): 17-22. https://doi.org/10.59298/NIJEP/2024/411722.1.1100