IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁑ Peer-reviewed & Refereed journal ⁑ Vol. 12, Issue 4, April 2024

DOI: 10.17148/IJIREEICE.2024.12433

A Review of IoT Applications, Attacks and Its Recent Defence Methods

Prof. Prachi Arihant Chougule[1], Prof. Supriya Arun Wadekar[2],

Prof. Shubhangi Shivaji Manjare[3]

Assistant professor, Electrical Engineering, DKTE Society's Textile and Engineering Institute, Ichalkarnaji, Maharashtra, India[1,2,3]

Abstract: In today's world, technology has seamlessly integrated into our daily lives. Particularly, the Internet of Things (IoT) has emerged as a convergence of diverse technologies across various application domains. The versatility of IoT applications spans across different environments. Consequently, safeguarding the security of IoT has emerged as a paramount concern. Recent observations highlight the susceptibility of IoT to sophisticated attacks, rendering services inaccessible to legitimate users. This study delves into IoT applications, focusing on IoT security, encompassing prevalent attack vectors and proposed solutions. Despite numerous solutions being offered, many come with inherent limitations and constraints. Identifying the most effective and dependable protective measures against sophisticated IoT threats remains a challenge. This review paper zeroes in on common and efficient strategies for fortifying the IoT ecosystem against cyber threats, encompassing both conventional and contemporary approaches. Furthermore, it outlines a framework and potential avenues for developing enhanced Distributed Denial of Service (DDoS) defence solutions.

1. INTRODUCTION

The concept of the Internet of Things (IoT) has garnered significant attention in recent years, with Kevin Ashton credited as its pioneer back in 1999. This surge in interest is fueled by remarkable advancements in mobile communication, Radio Frequency Identification (RFID), cloud computing, and Wireless Sensor Networks (WSNs), making communication among IoT devices more seamless than ever before [1]. Devices such as smartphones, laptops, PDAs, and other handheld embedded devices are integral components of the IoT ecosystem, relying on wireless communication networks to exchange valuable data with centralized systems [2].

Data generated by IoT devices undergoes centralized processing before dissemination to intended recipients. As a result, our daily lives increasingly interface with a virtual realm, thanks to the rapid evolution of communication and internet technologies [3]. While individuals can conduct activities like shopping, working, communicating, and even caring for pets and plants within this virtual environment, the fundamental reality remains that humans inhabit the physical world [4]. Thus, achieving complete automation of all human tasks proves to be a formidable challenge. Despite the potential for future advancements, the boundary of frictional space places constraints on the evolution of internet services.

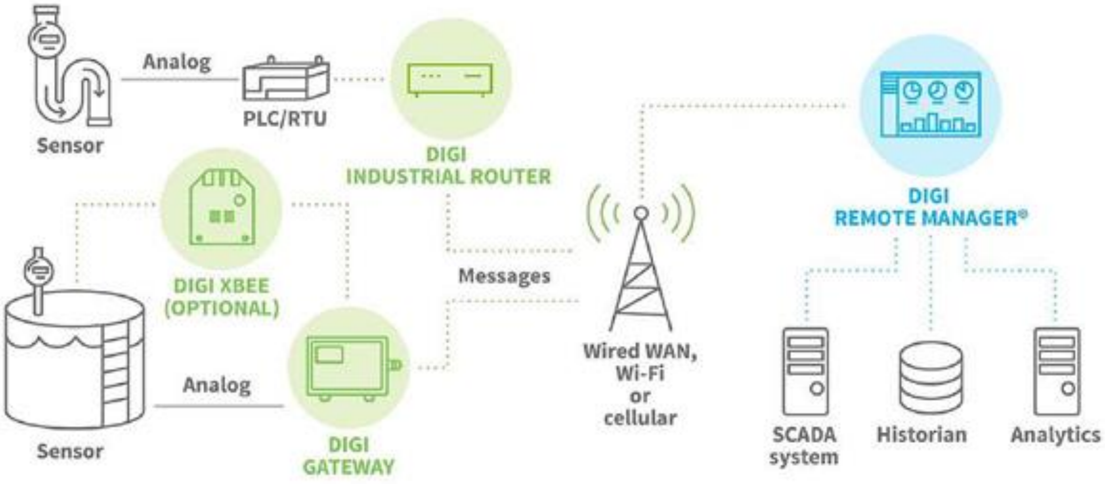

Fig. 1 the architecture of IoT environment [4], [7].

This work is licensed under a Creative Commons Attribution 4.0 International License

DOI: 10.17148/IJIREEICE.2024.12433

The IoT effectively merges the virtual and physical worlds onto a singular interface [5], driving a notable surge in the adoption of IoT devices, with an ever-growing number of devices connecting to the internet. Projections suggest a staggering 35 billion interconnected objects with approximately 300 billion connections by 2021, yielding revenues exceeding 800 billion euros. In China alone, the current nine billion connected devices are projected to reach 24 billion by 2020 [6]. This proliferation of IoT devices facilitates seamless communication between individuals and devices across diverse networks and services, transcending barriers of time and space [4], [7].

This study provides an in-depth exploration of the IoT landscape, outlining its applications and the prevalent types of attacks, alongside recent defense methodologies. Structured into four sections, the paper begins with an introduction elucidating the IoT environment, its applications, and the associated attack and defense mechanisms (Section 1). Section 2 delves into the intricacies of IoT applications, while Section 3 addresses IoT security measures. Finally, Section 4 offers concluding remarks on the study's findings.

2. IoT APPLICATIONS

The potential impact of the Internet of Things (IoT) on environmental and social dynamics is considerable as it evolves. Various IoT-based concepts, including smart grid systems, mobility solutions, smart buildings, public safety and medical applications, environmental monitoring, healthcare initiatives, and advancements in agriculture, hold promise for enhancing the human experience and creating a more sustainable future. However, despite the transformative potential, many IoT applications and devices lack robust defenses against confidentiality threats, giving rise to significant privacy and security concerns within IoT networks. These issues encompass challenges related to secrecy, identification, data integrity, and access control [5]. Attackers and intruders continuously target IoT devices, underscoring the urgent need for enhanced security measures.

Additionally, IoT finds application in diverse sectors such as industrial processing, animal breeding, and promoting independent living [8], each intertwined with our daily lives. The widespread use and reliance on IoT applications have reached visionary proportions in recent years, underscoring their indispensable role in shaping the future of the internet. Notably, the trajectory of the internet's evolution is profoundly influenced by the vision and concept of the Internet of Things, catapulting us toward a future where interconnectedness is ubiquitous [9].

In Figure 1, various IoT application domains are highlighted, demonstrating the breadth of its potential impact. This study focuses on elucidating the fundamental functional aspects of these applications, drawing on the extensive research conducted by scholars over the years. The versatility of IoT extends to various environments, as depicted in Figure 2, underscoring its adaptability and potential for widespread integration.

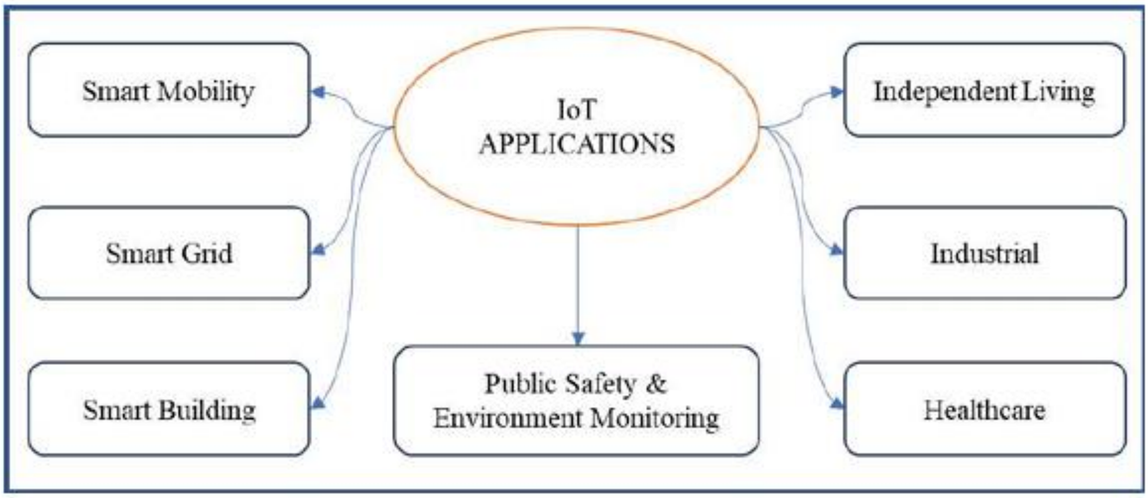

Fig. 2 The IoT Applications.

2.1. Smart Mobility

The methodology of smart mobility offers numerous avenues for access, evolving in efficiency and flexibility over time to meet the ever-growing demands of society. Within this framework, Vehicular Ad hoc Networks (VANETs) have garnered significant attention, representing a shift towards a more adaptable and multimodal transportation system.

© IJIREEICE This work is licensed under a Creative Commons Attribution 4.0 International License

DOI: 10.17148/IJIREEICE.2024.12433

VANETs serve as the cornerstone of the Internet of Vehicles (IoV), aimed at enhancing road safety, mitigating accidents, and introducing innovative solutions for optimizing transportation efficiency. Addressing challenges such as traffic congestion and facilitating seamless travel between locations remains a focal point of ongoing research and development efforts undertaken by experts in the field of mobility. These endeavors have led to the emergence of novel strategies grounded in contemporary resources [10].

2.2. Smart Grid

The Smart Grid employs digital communication technology to detect local fluctuations in electricity usage and responds accordingly. This two-way communication system between customers and utility companies enables customers to prioritize their energy consumption and demand. Energy is then distributed through the grid in accordance with the calculated requirements [11].

2.3. Smart Building

A Smart Building represents a residential space equipped with advanced technological amenities such as lighting, heating, and various other systems akin to traditional living environments. What sets these buildings apart is their capability to be remotely controlled via a smartphone or computer, a significant departure from conventional homes. The emergence of smart homes/buildings in recent years stems from the seamless integration of diverse technologies with the Internet [12].

2.4. The Public Safety & Environment Monitoring

The practice of vigilantly monitoring weather patterns, preserving endangered species, managing water resources, and other aspects directly or indirectly impacting our environment falls under the purview of public safety and environmental monitoring. This involves integrating applications with a range of sensors and observational equipment to promptly track changes in environmental factors [9].

2.5. Medical and Healthcare (IoMT)

The IoMT (Internet of Medical Things) encompasses a structured integration approach that links medical services with IT systems through interconnected computer networks. Medical devices are equipped with built-in Wi-Fi systems, facilitating machine-to-machine communication based on IoMT principles [1].

2.6. The Industrial Processing

In recent years, the Internet of Things (IoT) has surged in popularity within the industrial sector. The functionalities of IoT are tailored or developed to meet the specific demands of today's industrial equipment and requirements [13].

2.7. Independent Living

The concept of independent living aims to support older individuals in their daily routines, enabling them to lead self-reliant and secure lives. Significant scientific endeavors and contributions in this field have invoked the principles of IoT [14].

3. IoT SECURITY

As the landscape of IoT applications continues to expand and develop, attacks against these applications are becoming increasingly prevalent. Securing IoT devices poses a growing challenge for both manufacturers and consumers alike. Numerous studies have identified key security concerns, such as default or weak passwords, and the practice of storing data online without adequate password protection. Often, passwords used for IoT devices are simplistic, default, or sometimes nonexistent, creating vulnerabilities that jeopardize user security and enable hackers to orchestrate large-scale cyberattacks, including Distributed Denial of Service (DDoS) attacks using compromised IoT devices. For instance, Bashar et al. [7] reported a case where an unencrypted medical record containing information on 6 million individuals, including those in the United States and other regions, was publicly accessible [8].

3.1. The Most Common IoT Attacks

This section concentrates on the various types of attacks that could target the IoT environment, emphasizing the most prevalent and hazardous among them. Figure 3 illustrates the commonly encountered types of IoT attacks.

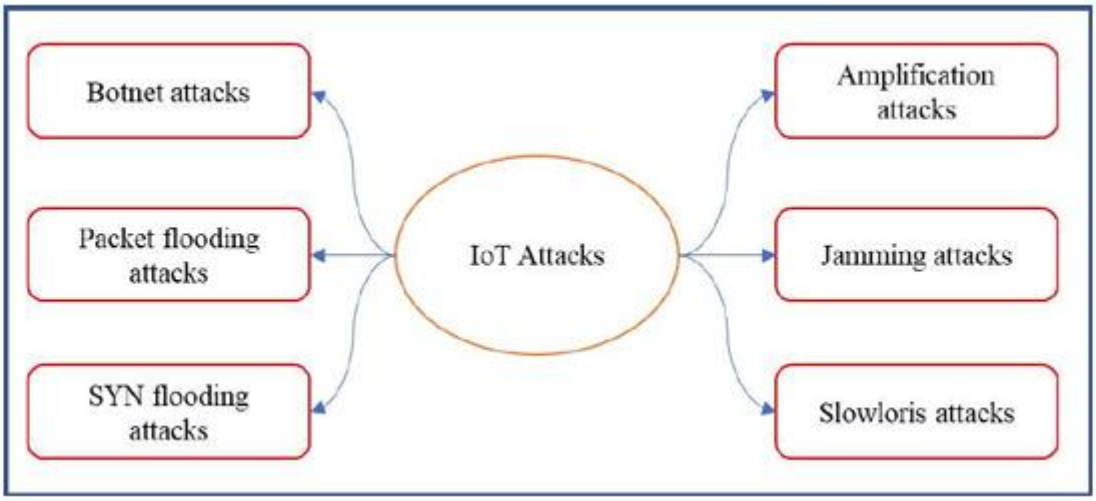

Fig 3: IOT attacks

3.1.1. Botnet attacks

The attacker utilizes compromised IoT devices, also referred to as bots or zombies, under the control of a handler. A botmaster, who is the hacker in charge of these bots, may employ various IP addresses to orchestrate large-scale attacks, such as sending spam emails for financial gain or launching Distributed Denial of Service (DDoS) attacks on critical infrastructure or websites, rendering them inaccessible. In 2016, one of the most notorious large-scale IoT botnet attacks, "Mirai," caused high-profile websites like the New York Times, Twitter, Netflix, GitHub, and others to become unavailable [7].

3.1.2. Packet flooding attacks

Another type of large-scale assault is packet flooding, which occurs because web hosts lack control over the packets they receive [7], [8]. Since IoT devices have internet connectivity, they are susceptible to flooding attacks, and IoT traffic may traverse multiple hops before reaching a gateway or an Intrusion Detection System (IDS). The sequence of routers that packets travel through is not included in packets received at a router. Attackers can exploit this by falsifying the Internet Protocol (IP) and inundating the victim with counterfeit packets, causing the victim's system to crash. An example of a flooding attack is UDP flooding, where UDP datagrams flood the network, causing congestion [8]. Another tactic is ICMP flooding, wherein a continuous stream of ping packets is broadcast to the recipient without receiving a response, thereby overwhelming network resources.

3.1.3. SYN flooding attacks

In a SYN flooding attack, the conventional TCP three-way handshake protocol is exploited. The attacker employs fake IP addresses to send numerous SYN packets to various ports on the target. Typically, when the destination responds to the SYN request with a SYN-ACK message, the source should reply with the intended ACK message. However, in this attack, the source rarely responds, causing the target to remain in a waiting state for a response until its connection limit is reached or it times out. This prevents the target from responding to genuine requests [8].

3.1.4. Slowloris attacks

Slowloris is a type of DDoS attack that specifically targets HTTP servers. This method involves opening numerous HTTP connections to the target web server. By sending incomplete and continuous HTTP requests, these connections are kept open indefinitely. The targeted web server keeps these connections open, gradually depleting its resources until they are completely exhausted [6]. Slowly penetrating DDoS attacks are challenging to detect.

3.1.5. Jamming Attacks

Jamming attacks pose significant threats to IoT devices as they can rapidly drain battery capacity by disrupting data transmission and frequently retransmitting it [8]. These attacks are particularly perilous for the IoT ecosystem due to the resource limitations of IoT devices. Jamming attacks detrimentally affect distributed systems by interrupting communication, diminishing IoT performance, halting communication altogether, and depleting the limited energy resources of IoT devices [1], [8].

DOI: 10.17148/IJIREEICE.2024.12433

3.1.6. Amplification Attacks

In amplification attacks, adversaries augment the force of the assault. Attackers execute these attacks by exploiting protocol vulnerabilities and impersonating source IP addresses. Examples of amplification attacks include DNS amplification, ICMP amplification, and UDP amplification [6].

4. THE PROPOSED SOLUTION

Numerous solutions have been proposed to safeguard the IoT environment against cyber-attacks. However, in this section, we provide a summary of the most common and effective solutions, as depicted in Figure 4 below.

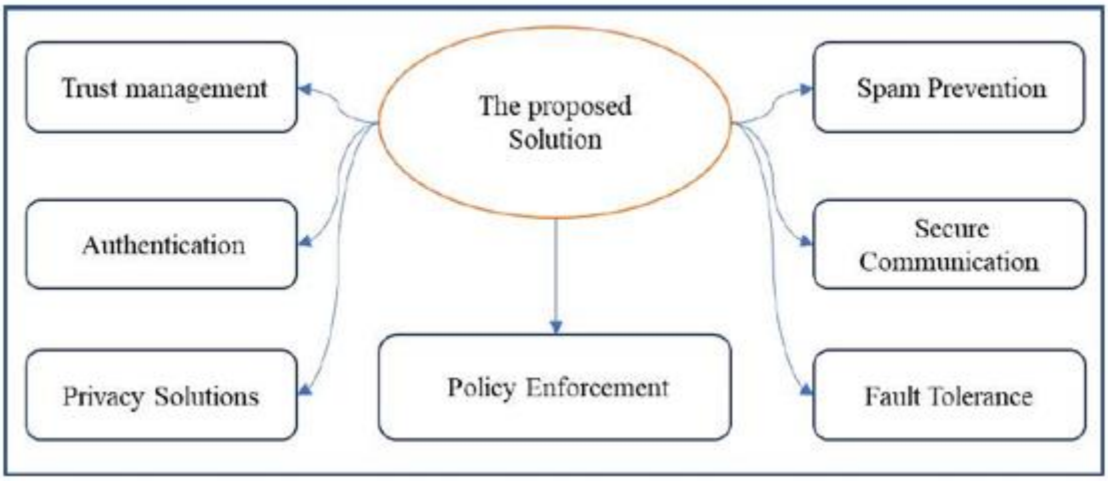

Fig. 4 The most effective defense methods.

4.1. Trust Management

Trust management plays a pivotal role in IoT security, as highlighted in research by [6]. Utilizing trust managers can aid individuals in navigating the risks and uncertainties associated with the Internet of Things. Trust encompasses both privacy and security aspects and is recognized as a fundamental requirement for IoT systems [7]. Authors in [15] also emphasize that trust is contingent on users' interactions with IoT devices, underscoring the importance of empowering consumers to manage their resources and understand their engagements with IoT systems. Effective management practices contribute to fostering trust in IoT environments.

4.2. Authentication

Implementing various authentication mechanisms for IoT can enhance data security and privacy. Previous works by authors [6, 15] illustrate authentication approaches to bolster IoT security and privacy. Authentication methods may include gateway security tokens, global trust trees, or trust chains, each with its own set of advantages and disadvantages. In [56], a two-level key management session is proposed for IoT end-user authentication, contributing to the development of a session key-based authentication method for IoT security.

4.3. Privacy Solutions

Addressing privacy concerns in IoT requires a multifaceted approach. Innovative solutions for privacy challenges are proposed in previous work [16], advocating for user-managed data tools. Privacy by design principles emphasize integrating privacy considerations into the design process, while transparency principles highlight the importance of consumers understanding how their data is handled. Data management strategies and policy enforcement methods are crucial for privacy solutions.

4.4. Policy Enforcement

Policy enforcement is deemed essential for addressing security issues in IoT environments. Research [17] focuses on software-based solutions for IoT security, presenting a security architecture solution comprising micro security functionalities known as boxes. This architecture includes a centralized IoT Sec controller capable of monitoring the environment and establishing a common understanding of cross-technology implementations, enabling network managers to configure innovative boxes and transmission techniques based on this understanding.

DOI: 10.17148/IJIREEICE.2024.12433

4.5. Fault Tolerance

Proposals for fault-tolerant IoT systems aim to meet diverse requirements. Research by [16] emphasizes safeguarding IoT through innovative solutions to address the escalating number of assaults on the Internet and its devices. Their methodology outlines conditions for IoT devices to achieve fault tolerance, including ensuring initial security settings, continuous monitoring of devices and networks, and enabling devices to protect themselves against network outages and threats, ensuring quick response and recovery in the event of service disruptions [7].

5. CONCLUSION

Taking into account the value, volume of devices, and data generated by interconnected devices, known as IoT, enables merchants and organizations to devise efficient solutions that can scale, safeguard their data, and operate optimally in this burgeoning data-driven IoT industry. It also facilitates understanding various trends in data consumption, utilization, and storage. However, concerns regarding public and private safety, including confidentiality, accessibility, and integrity, among others, have hindered the rapid, robust, and widespread adoption of IoT, despite its immense potential.

REFERENCES

[1]. Abiodun, O. I., Abiodun, E. O., Alawida, M., Alkhawaldeh, R. S., & Arshad, H. (2021). A review on the security of the internet of things: challenges and solutions. Wireless Communications, 119(3), 2603-2637.

[2]. Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. Computers & Security, 112, 102494.

[3]. Sivapriyan, R., Sushmitha, S. V., Pooja, K., & Sakshi, N. (2021, December). Analysis of Security Challenges and Issues in IoT Enabled Smart Homes. In 2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS) (pp. 1-6). IEEE.

[4]. Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010, August). Research on the architecture of Internet of Things. In 2010 3rd international conference on advanced computer theory and engineering (ICACTE) (Vol. 5, pp. V5-484). IEEE.

[5]. Hua, W., Dai, F., Huang, L., Xiong, J., & Gui, G. (2019). HERO: Human emotions recognition for realizing intelligent Internet of Things. IEEE Access, 7, 24321-24332.

© IJIREEICE This work is licensed under a Creative Commons Attribution 4.0 International License