https://africanjournalofbiomedicalresearch.com/index.php/AJBR
Afr. J. Biomed. Res. Vol. 28(2s) (February 2025); 517-522
Research Article

Analysis of Security in IoT: Risks and measures with impact of emerging technologies

Divyansh Shrivastava[1*], Kalaivani K[2], Tilak Sharma[3]

[1*]Department of Computer, Science & Engineering Vellore Institute of Technology Vellore, Tamil Nadu, India, divyansh.prashant2021@vitstudent.ac.in

[2]School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India kalaivani.k@vit.ac.in

[3]Department of Computer, Science & Engineering Vellore Institute of Technology Vellore, Tamil Nadu, India, tilak.sharma2021@vitstudent.ac.in

***Abstract*—** The Internet of Things (IoT) is defined as a network of physical things that include cars, appliances, and other devices, that are equipped with sensors, software, and having network connectivity. The IoT devices can gather and exchange data among themselves. Smart cities, intelligent transportation, and healthcare are just a few of the applications that have greatly changed daily life as a result of the Internet of Things' (IoT) explosive expansion. However, IoT systems are increasingly prone to different security risks due to the diverse and heterogeneous nature of devices and the lack of standardization in security measures. This study examines the risks and difficulties that Internet of Things applications must overcome, with an emphasis on the possibility of cyberattacks that could specifically target low-resource devices. It examines typical attack vectors and explores lightweight security solutions targeted at boosting device safety while keeping performance. In order to enable the safe deployment of IoT technology in everyday situations, the paper emphasizes how important it is to solve these security challenges.

Keywords: IoT, Cyber-attacks, Security Challenges, Lightweight Solutions, Open Issues.

***Author of correspondence: Email:** *divyansh.prashant2021@vitstudent.ac.in*

Received 21/01/2025, Acceptance 05/02/2025

DOI: https://doi.org/10.53555/AJBR.v28i2S.6709

I.INTRODUCTION

In 1999, Kevin Ashton of Procter & Gamble coined the phrase "Internet of Things" (IoT), which refers to a paradigm of communication [1]. The Internet of Things is expanding quickly and becoming more and more popular in a wide range of common applications, including washing machines, microwave ovens, smart lamps, and televisions, to mention a few. Every item or gadget in the Internet of Things (IoT) is widely connected to and communicates with other items because to its ease of use and deployment. Wireless Sensor Networks (WSNs) and Radio Frequency Identification (RFID) are used to connect the virtual and physical worlds. Additionally, these gadgets have sensors that are crucial for detecting occurrences, gathering data, and sending it to networks via the internet to networks for processing and decision-making [2].

It is anticipated that by 2022, there will be twice as many IoT devices online as there were in 2016, with a total of 30 billion in 2016. Nonetheless, the general public still does not have a broad understanding of IoT services. Strong security measures are urgently needed in the IoT ecosystem due to the growing number of connected

devices and the increase in cyberattacks [3][4]. To avoid data breaches, theft, and integrity loss, IoT developers must be proactive in creating secure devices. IoT is an extension of the internet, much like computers, in which different things—including people, animals, cars, logistical equipment, and home appliances—are linked and reliant on one another.

The Internet of Things (IoT) is growing quickly, with 20.8 billion devices predicted to be online by 2020, according to projections made by Gartner Inc. [5]. Sensors and actuators that make use of short-range communication technologies, such as Near-Field Communication (NFC), Bluetooth, Zigbee, wireless communication, 6LoWPAN, and Machine-to-Machine (M2M) protocols, are essential to this extensive interconnectedness between the physical and virtual worlds. Smart homes, smart grids, healthcare, transportation, aviation, oil and gas, manufacturing, wastewater management, robotics, and agriculture are just a few of the many IoT applications that have surfaced in recent years, as shown in Figure 1.

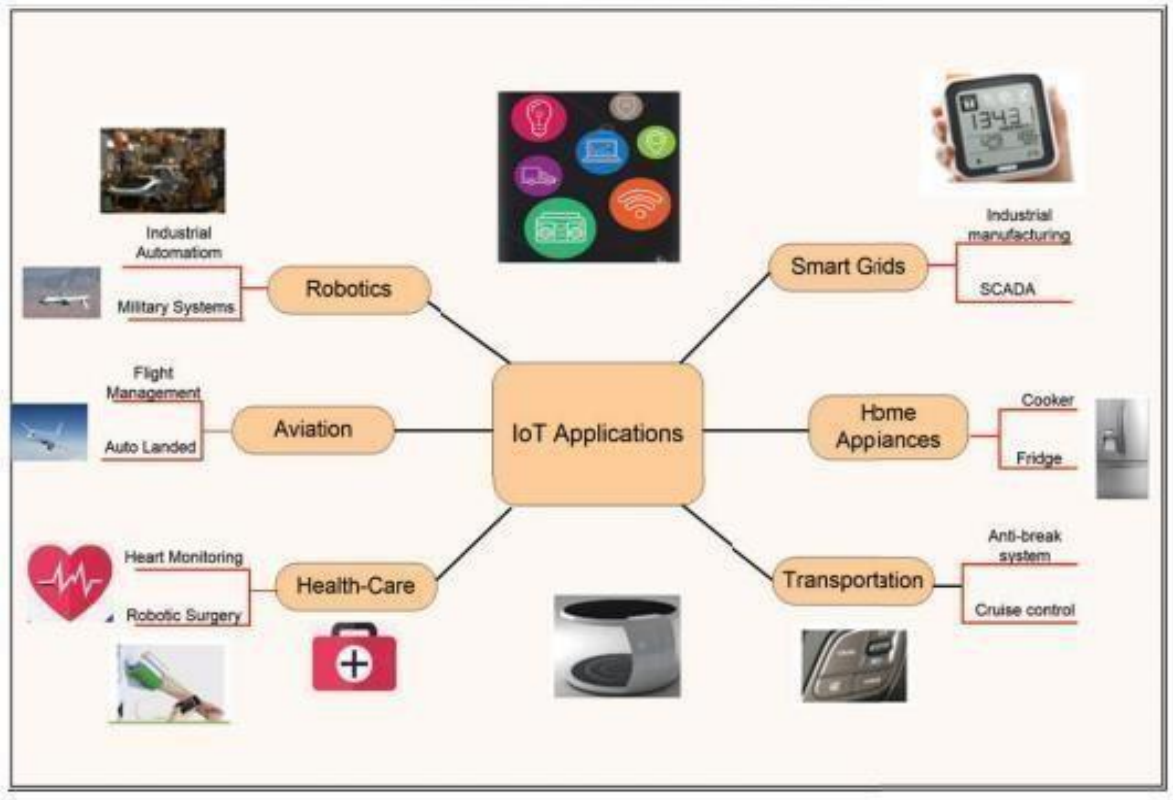

Figure.1

The goal of this paper is to present a thorough and in-depth analysis of the security threats related to Internet of Things (IoT) devices. It is intended to give all parties involved—from organizations and individual users to legislators and technologists—the fundamental knowledge they need to successfully negotiate the constantly changing IoT security environment. In addition to analyzing the intricacy of these threats, the article provides a roadmap for improving IoT ecosystem security by describing methods for successfully reducing them.

II.PROPOSED SECURITY SOLUTIONS

A flexible and adaptable security architecture is necessary to address the many and different security concerns that exist in the IoT ecosystem. Many IoT frameworks and standards have been created in recent years to help developers create products that satisfy the wide range of user needs [6]. Four essential elements make up the security framework for IoT shown in Figure 1, which is intended to address these issues:

- Network Policy
- Authentication
- Authorization
- Secure Analysis
- Control and Visibility
- Minimization of data

***Authentication*:**

level, which is used to confirm and establish the identification of an IoT device, is the fundamental component of the architecture of an IoT system. When a gadget has to connect to the Internet of Things network, its identification forms the basis of trust. diverse IoT devices may store and display this identifying information in very diverse ways. RFID, shared secrets, X.509 certificates, the MAC address, or hardware-based trust methods are frequently used identifiers for IoT devices since they need to be authenticated without the need for human contact. Public keybased activities are difficult in this situation because, although X.509 certificates provide a robust authentication scheme, IoT devices sometimes lack the capacity to store such

certificates or the computing power to carry out the cryptographic operations required for their validation.

Authorization:
the second layer of this security system, controls a device's network access control. This layer uses the device's identity information to enhance the authentication process. Authorization and authentication work together to establish a trustworthy connection between IoT devices, enabling safe information exchange.Forexample, two vehicles from the same manufacturer can establish a reliable connection and share safety-related information. However, only certain information, such safety features, could be shared due to this trust connection. The car might be allowed to communicate further information, such its mileage or maintenance history, when a secure connection has been made between it and the dealer's network.
Thankfully, consumer and business networks' current access management and control solutions are built to accommodate IoT requirements. Creating an architecture that can handle billions of IoT devices, each with unique trust relationships, is the primary problem. Traffic controls will be put in place throughout the network to separate data traffic and guarantee safe, end-to-end connectivity in order to solve this.

Networks Policy:
This layer includes all of the services that safely steer and manage traffic, including as management, control, and real data flow. Like the authorization level, there are already established protocols and processes in place to safeguard the network infrastructure and apply suitable policies for different use cases of the Internet of Things.

Secure Analysis:
Control and Visibility The services that offer telemetry—which gives insight and control over the Internet of Things network—are the main focus of this layer. The development of data systems has made it possible to process massive amounts of data in real time using a parallel database platform (MPP), which improves network visibility and administration.

Minimization of data:
Organizations utilize data minimization as a way to control their data by establishing the duration of retention. Organizations that gather personal data should follow the data reduction principle as part of their security and privacy procedures. This implies that they should only gather the information required for a particular use and for a brief period of time, and then safely discard it thereafter. Keeping a lot of data can make data breaches more likely.

III.IOT THREAT ANALYSIS

Three primary categories can be used to classify IoT security threats. The first consists of hardware-focused attacks, like those that impact integrated circuit (IC) applications. Threats from malicious software that aims to take complete control of devices fall under the second category. Threats that intercept and modify data during transmission fall under the third category. These dangers can be divided into two categories:

Hardware threats
Software threats

Hardware threats:
Hardware Trojan – This occurs when an attacker observes, alters, or disables the data stored in a circuit or the communication within the circuit through a trojan. This can happen during the design or manufacturing phase of the device. In [12], hardware trojans are categorized into:
• Combinational: The trojan activates when a specific condition is met at certain points in the circuit.
• Sequential: The trojan triggers after a specific sequence of rare logic values occurs at certain points in the circuit.
• Attributes: These include physical characteristics, activation methods, and actions.
• Trigger and Payload Mechanism: The trigger mechanisms can be either digital or analog.
Side Channel Attack – This type of attack happens when an attacker takes advantage of the physical information leaks from a system during an application's execution. The attacker conducts non-invasive, hardware-based attacks by observing and measuring things like power usage, electromagnetic radiation, timing, and sound. This gathered data can be analyzed to steal private information like cryptographic keys. Examples of side channel attacks include differential fault analysis [13], power monitoring attacks [14], electromagnetic analysis attacks [15], and acoustic cryptanalysis [16].
• Tampering – This is when an attacker changes the data of an integrated circuit (IC) after it has been used in an application. Many IoT devices are placed in environments without physical protections, allowing attackers to gain physical access to the device or wirelessly manipulate its software or firmware. An attacker may install malicious hardware or software to alter the IC's behavior.
• Denial of Service (DoS) or Distributed DoS (DDoS) – In this case, attackers interfere with the internal structure of an IC to prevent users from accessing its services.

Software threats:
• Botnet – These are devices infected with malicious software and connected to the internet. IoT devices often have weak security, making them easy targets for cyber-criminals. Once infected, these devices become part of a botnet, which the attacker controls. Cyber-criminals use botnets for phishing, spamming, spreading malware, and carrying out Distributed Denial of Service (DDoS) attacks. The botnet structure can be peer-to-peer, centralized, or a combination of both.
• Spoofing – This happens when an attacker pretends to be a legitimate IoT device or user to gain unauthorized access to a network. The attacker typically uses the legitimate user's Media Access Control (MAC) address or Internet Protocol (IP) address.
• DoS – In a Denial of Service (DoS) attack, attackers use one or more computers to overwhelm a target with excessive data or messages, causing a disruption in

service. Some common DDoS attacks include UDP Flood, ICMP (ping) Flood, SYN Flood, Ping of Death, Slowloris, NTP Amplification, HTTP Flood, and zero-day DDoS attacks.

Common issues including illegal access, the value of encryption, and physical security flaws are shown by the literature on IoT device security. These problems are interrelated, as seen by the intricacy of various communication protocols and the requirement for uniform security measures. Supply chain security is now acknowledged as a major concern, and security is increasingly perceived as a complex issue requiring an all- encompassing strategy. Case studies illustrate how inadequate security affects people in the real world. This paper offers a thorough analysis of the security threats associated with IoT, highlighting the necessity of standardized frameworks and pointing out areas that require more investigation. Creating efficient mitigation techniques to improve IoT security will be the main goal of the following stage.

Due to their ongoing internet connectivity, IoT devices are susceptible to possible cyberthreats and can be exploited by cybercriminals.

Botnet Use:

Botnets are frequently used in cybercrimes such malware distribution, spamming, and phishing. When compromised, Internet of Things (IoT) devices can play a crucial role in a distributed denial-of-service (DDoS) attack. These botnets include Kaiten, Spike, and Mirai. In order to create a network of bots that can be used for malevolent purposes, these botnets take over weak Internet of Things devices, such cameras and routers, whose security is frequently disregarded or ignored.

Reasons for IoT Attacks:

Due to a number of flaws, such as default software setups, erratic software updates, and the protracted interval between security patch releases and installation, cybercriminals can readily target IoT devices. Using the default login credentials, which are frequently left unaltered, to gain access to devices is a typical attack. The Mirai botnet, for instance, compromised several devices using this technique. Changing the factory-default usernames and passwords can reduce the danger of such assaults.

The usage of botnets in ransomware attacks is another serious security issue. Devices are locked and encrypted during these attacks, and access is only unlocked if a ransom is paid. Furthermore, intrusion detection systems (IDS) are essential for protecting Internet of Things (IoT) devices from dangers such as Distributed Denial- of-Service (DDoS) assaults. Telnet, a common target for assaults, is used to connect many IoT devices. Without adequate security, devices can be scanned for vulnerabilities using programs like Zmap and Nmap. The probability of such cyberattacks can be decreased by putting intrusion detection systems into place. [7-10]

Security of networks:

Protecting networks is the biggest challenge in the Internet of Things (IoT) space because of the numerous protocols that are employed and the distinctions between wired and wireless communication standards.

Authentication:

Appropriate authentication is necessary when managing numerous users on a single device. Static passwords are vulnerable to spoofing and don't offer the required protection. Stronger authentication techniques, such as digital certificates, two-factor authentication, and biometrics, are therefore necessary for reliable breach protection. It's also crucial to remember that the approval procedure usually depends only on machine-to-machine (M2M) communication and excludes human intervention.[11] *The use of encryption:*

Standardized encryption techniques and algorithms, as well as efficient key management, are essential for preserving data integrity and thwarting hacker invasions. The general security of IoT devices may be jeopardized by inadequate key management. [11]

IV.CURRENT PROBLEMS, DIFFICULTIES, AND FUTURE DIRECTIONS FOR RESEARCH

The Internet of Things, or IoT, is now growing quickly and has several advantages for both individuals and the IT sector. IoT does, however, confront a number of security concerns and difficulties that must be addressed despite its notable rise. Because the IoT architecture is made up of several layers, each of which has a different set of devices, communication channels, and protocols, there are many different and intricate security concerns and threats. Furthermore, trust is necessary for the interactions between these layers and the devices involved, but it can be hard to build and simple to undermine in the absence of adequate controls and safeguards.

The absence of a consistent framework that guarantees end-to-end security is another crucial problem that is frequently disregarded. Furthermore, the threat landscape is changing as a result of developments in information and communication technologies (ICT), including data science and machine learning. Attackers are using more and more creative methods to get beyond the security measures in place. Because of this, security concerns must be taken into account and implemented at every stage of IoT design and operation.

Among the major issues that require attention are:

Identity management and authentication Protection of Privacy Trust Management and Data Security Architectures of Software and Hardware It is evident from the aforementioned study that specific security concerns are necessary due to the various and heterogeneous character of the Internet of Things. New, strong countermeasures and frameworks that guarantee complete, end-to- end security throughout the IoT ecosystem are desperately needed. Additionally, cooperation between various IoT layers—for example, by putting cross-layer security solutions into place—can aid in resolving integration issues and enhancing scalability

V. DISCUSSION

We learned from this study that designing the Internet of Things (IoT) to be both user-friendly and secure is essential. One major issue with deploying IoT in many contexts is security. The fundamental tenet of the Internet of Things is to link everything to the worldwide Internet so that gadgets may speak with one other remotely. This raises fresh security issues regarding the privacy, accuracy, and legitimacy of the data transferred between Internet of Things devices. We came to the conclusion that more study is required with an emphasis on creating strong security features in IoT systems in order to prevent unwanted access to sensitive data while still permitting authorized users to exchange and access data. We came to the conclusion that more research is required to concentrate on creating strong security features in IoT systems in order to stop illegal access to private data while still permitting authorized users to exchange and access data. Using encryption methods that satisfy security requirements while reducing processing time is necessary to ensure data confidentiality, integrity, and validity. In conclusion, IoT security is important, fraught with difficulties, and necessitates simple, workable solutions that blend seamlessly into everyday applications

VI. CONCLUSIONS

The security risks and difficulties that IoT devices and apps face are reviewed in this article. IoT necessitates specific security measures in addition to new methods and countermeasures because of the variety of devices and settings. It draws attention to the advantages of Internet of Things applications as well as the kinds of risks they encounter. Customized security solutions are required to reduce attack damage and fully profit from IoT. Additionally, the article highlights the importance of addressing fundamental security weaknesses in devices by illustrating vulnerabilities in wireless technology through two attack cases. Manufacturers must concentrate on enhancing security as IoT expands because the present user protection initiatives are inadequate. Businesses must constantly update their attack detection systems to handle changing threats until manufacturers offer strong defenses. IoT devices will continue to be vulnerable and be used if they are not properly treated for malicious purposes.

VII. REFERENCES

[1] M. G. Samaila, M. Neto, D. A. Fernandes, M. Freire, and P. R. Inácio, “Challenges of securing internet of things devices: A survey,” Security and Privacy, vol. 1, no. 2, p. e20, 2018.

[2] W. H. Hassan et al., “Current research on internet of things (iot) security: A survey,” Computer Networks, vol. 148, pp. 283–294, 2019.

[3] `J. Sonnerup, J. Karlsson, "Robust Security Updates for Connected Devices", pp. 105, March 2016.

[4] Emmanuel BACCELLI et al., "OS for the IoTGoals Challenges and Solutions", Workshop Interdisciplinaire sur la Sécurité Globale (WISG2013), 2013

[5] L. S. Sayana and B. K. Joshi, “Security issues in internet of things,” Uttarakhand: ICFAI, 2016.

[6] Liu, Xiruo, et al. "A security framework for the internet of things in the future internet architecture", 2017, pp. 27

[7] Dhanush V, Mahendra A R, Kumudavalli MV,Debabrata Samanta , Application of deep learning technique for automatic data exchange with Air-Gapped Systems and its Security Concerns, Proc. of IEEE International Conference on Computing Methodologies and Communication [ICCMC 2017], pp. 324 - 328, @IEEE , 18-19, July 2017 , Erode. DOI: 10.1109/ICCMC.2017.8282701

[8] R Kumar, Rishabh K,Debabrata Samanta , M Paul, CM Vijaya Kumar, A Combining approach using DFT and FIR filter to enhance Impulse response, Proc. of IEEE International Conference on Computing Methodologies and Communication [ICCMC 2017]pp. 134 - 137, @IEEE , 18-19, July 2017 , Erode.DOI: 10.1109/ICCMC.2017. 8282660

[9] G Ghosh, Debabrata Samanta, , M Paul, N Kumar Janghel, Hiding Based Message Communication techniques depends on Divide and Conquer Approach, Proc. Of IEEE International Conference on Computing Methodologies and Communication [ICCMC 2017], pp. 123 - 128, @IEEE , 18-19, July 2017 , Erode. DOI: 10.1109/ICCMC.2017.8282658

[10] R. K. Singh, T. Begum, L. Borah, Debabrata Samanta, Text Encryption: Character Jumbling, Proc. of IEEE International Conference on Inventive Systems and Control [ICISC 2017],pp. 1 - 3, @IEEE , 19-20 January 2017 ,Coimbatore. 978-1-5090-4715-4/17/$31.00 @ 2017 IEEE. DOI: 10.1109/ICISC.2017.8068691

[11] M. Humayun, M. Niazi, N.Z. Jhanjhi, M. Alshayeb, S. Mahmood, Cybersecurity threats and vulnerabilities: A systematic mapping study, Arab. J. Sci. Eng. 45 (4) (2020) 3171–3189.

[12] S. Simranjeet, J.M. Bassam, H. Thaier, Hardware security in IoT devices with emphasis on hardware trojans, J. Sensor Actuator Netw. 8 (3) (2019) 42

[13] J. Breier, W. He,. “Multiple fault attack on PRESENT with a hardware Trojan implementation in FPGA.” In Proceedings of the IEEE International Workshop on Secure Internet of Things (SIoT), Vienna, Austria, 21–25 September. 2015; pp. 58–64.

[14] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury and S. Sen, "High efficiency power side-channel attack immunity using noise injection in attenuated signature domain," 2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA, 2017, pp. 62-67.

[15] W. Zhou and F. Kong, "Electromagnetic side channel attack against embedded encryption chips," 2019 IEEE 19th International Conference on Communication Technology (ICCT), Xi’an, China, 2019, pp. 140-144 [16] D. Genkin, A.

Shamir, E. Tromer, Acoustic cryptanalysis, J. Cryptol. 30 (2017) 392

[17] I. Ullah, N. Khan and H. A. Aboalsamh, "Survey on botnet: Its architecture, detection, prevention and mitigation," 2013 10th IEEE International Conference on Networking, Sensing and Control (ICNSC), Evry, 2013, pp. 660-665.