Volume: 14 Issue: 03 Pages: 5444-5454(2022) ISSN: 0975-0290

# Internet of Things (IoT) Security: Status, Challenges and Countermeasures

**Navod neranjan thilakarathne**
Department of ICT, Faculty of Technology, University of Colombo, Sri Lanka
Email: navod.neranjan@ict.cmb.ac.lk
**Rohan Samarasinghe**
Department of ICT, Faculty of Technology, University of Colombo, Sri Lanka
Email: rohan@ict.cmb.ac.lk
**DMCK Dasanayake**
Department of ICT, Faculty of Technology, University of Colombo, Sri Lanka
Email: 2019t00436@stu.cmb.ac.lk
**M.F.F. Fasla**
Department of ICT, Faculty of Technology, University of Colombo, Sri Lanka
Email: 2019t00441@stu.cmb.ac.lk
**AMSD. Ananda**
Department of ICT, Faculty of Technology, University of Colombo, Sri Lanka
Email: 2019t00470@stu.cmb.ac.lk
**G.H. Sonnadara**
Department of ICT, Faculty of Technology, University of Colombo, Sri Lanka
Email: 2019t00471@stu.cmb.ac.lk
**M.T. Sahirullah**
Department of ICT, Faculty of Technology, University of Colombo, Sri Lanka
Email: 2019t00465@stu.cmb.ac.lk
**R.G.T.R.L. Wijesekara**
Department of ICT, Faculty of Technology, University of Colombo, Sri Lanka
Email: 2019t00475@stu.cmb.ac.lk
**DSD. Silva**
Department of ICT, Faculty of Technology, University of Colombo, Sri Lanka
Email: 2019t00470@stu.cmb.ac.lk

----------**ABSTRACT**----------

**The Internet of Things (IoT) is a vast concept spreading rapidly throughout the world today. Due to their inherent nature, IoT devices are more vulnerable to attacks than other cyber infrastructure. In a typical IoT system, four different types of layers can be identified. Those layers can be specified as the application layer, data processing (software) layer, network layer, and sensing (physical) layer. According to this architecture, each layer operates under different technologies. Thus, various challenges and vulnerabilities related to security have emerged and exist. Thereby extant and forthcoming IoT applications must comply with standard cyber security guides and regulations to guarantee safety; otherwise, they would jeopardize the lives of people using these IoT applications resulting in chaos. To achieve this, IoT applications can create environments with end-to-end security by adding security measures and the required adjustment, guaranteeing safety and privacy. By bearing this in mind, this research reviews the different types of security challenges, such as access control attacks and physical security attacks found in each of the four layers of the IoT architecture, along with what countermeasures can be taken to mitigate these attacks. As the main objective of this research is to examine underlying security challenges in the standard IoT architecture, we examine and categorize IoT vulnerabilities and outline methods used to ensure such IoT systems safety. Further, we also present the future directions in terms of security and privacy of IoT as well.**

Keywords - **Cybersecurity, Encryption, Internet of Things, IoT, Protocols, Security, Sensors, Internet, Wireless Sensor Networks**

Date of Submission: Sep 21, 2022 Date of Acceptance: Oct 17, 2022

## I. INTRODUCTION

Over the years, various technologies have been developed to accomplish different tasks towards making our life easy. IoT is a fast-growing and pervasive technology that has showcased exponential growth in recent years. According to the latest research, the total number of interconnected IoT devices is expected to be more than 30 billion by 2025 [1]-

[3]. In the past century, the world has achieved tremendous milestones owing to the contributions of Information and Communication Technologies (ICT). Now the place of this ICT has been acquired by the IoT,

Volume: 14 Issue: 03 Pages: 5444-5454(2022) ISSN: 0975-0290

with the immense benefits they contributed to the development of various industries such as healthcare, agriculture, smart cities, and so on [4]-[8].

IoT is generally referred to as an interconnected, widely spread network of smart devices or embedded devices (things) connecting through the Internet. It primarily designs an enormous geographically distributed network that connects many devices to gather data, manipulates data, sometimes processes that data, and uses that processed data to make intelligent and smart decisions by exchanging information [9]-[12]. These IoT physical objects or things include devices such as smart virtual assistants, smart meters, smart home cleaners, smart lights, smart glasses, and other home appliances used in day-to-day life and as well as heart-rate detectors, smart thermometers, parking sensors on cars, Logix controllers and other smart industrial devices [3],[13]-[16]. On the other hand, IoT also includes different sensor-embedded devices, wired, wireless, private, or public communication networks, and sensor networks such as Wireless Sensor Networks (WSN). Further IoT enables people and devices to connect through the Internet with any other people and devices, anywhere and anytime [4],[5],[17]-[20].

The concept of interconnected devices was first proposed in 1832 when Baron Schilling invented the first electromagnetic telegraph [6],[20]-[24]. In 1982, students at Carnegie Mellon University designed the first connected devices for a Coca-Cola vending machine to monitor the machine's contents [7],[8],[25]-[29]. Later the advancement of the World Wide Web (WWW) in 1989 fueled the growth of IoT and paved the way for the wide use of IoT. The term “Internet of Things” was created in 1999 and introduced by Kevin Ashton [30]-[35].

In 2010, the IoT paradigm started to take off high owing to the increased adoption of IoT in various industries making every IoT infrastructure target for cyber-criminals if they are not secured well[8]-[12]. As of now, this IoT security has become a critical problem for governments, companies, and individuals to protect their networks from cyber attackers.

On the other hand, cybercriminals are taking advantage of the coronavirus threat to increase their attacks on remote workers and connected devices making the situation worse. Almost every industry is at risk with IoT, as 92% of industrial businesses, 82% of healthcare organizations, and 63% of corporations use IoT [13]. IoT systems and technologies are still evolving, yet there are many challenges to overcome, among which security is the most important [36]-[40].

In this research, we aim to provide a brief review of security threats that target IoT and measures that can be taken to prevent them. In this regard, the rest of the paper is structured as follows. Following the introduction, section two provides a brief background of the IoT security challenges, security challenges in terms of its layered architecture, and real-world examples of security attacks. In section three, we discuss countermeasures that can be taken. Section four highlights anticipated future directions regarding IoT security, and finally, the paper concludes with the conclusion.

## II. IOT SECURITY CHALLENGES

The security impact of IoT extends from our homes to our offices and beyond. Every day we access and deal with our highly sensitive and personal data through various IoT devices. As every device in the user’s environment has sensors with other components connected to the Internet, hackers can easily intrude through the Internet. Hence everything from wired and interconnected devices to IoT over wireless networks produces a large attack surface for cyber attackers [14]-[18],[40]-[45]. With advanced hacking techniques and tools, attackers are now capable of completely crashing or crippling a system. Therefore, users’ trust and interest in IoT may eventually be diminished. Thus, IoT users also have responsibilities associated with certain functions of the IoT as they are the main stakeholders using these devices. For example, using accurate and secure devices and regularly updating information such as user credentials is essential for preventing attacks [19]-[23].

IoT security threats can cause extensive damage to IoT infrastructure, resulting in the loss of lives of people using it. According to the literature [4]-[8],[46]-[50], these threats and challenges can be apportioned according to the layered architecture of IoT [20]-[24]. Hence, considering all these aspects, IoT security challenges can be identified in four ways: local, network, software, and hardware security challenges [23]-[28].

### *A. Why is IoT security important?*

Over the last decade, cyber-attacks that target IoT have rapidly increased owing to the wide use of IoT [29],[30],[50]-[53]. According to the latest research [30]-[35]; it is evident that 70% of televisions, web cameras, home-based alarm systems, televisions, door locks, and other devices use network services that are not encrypted, posing a doubt about securing user data [36]-[40]. On the other hand, when we consider the 2020 and 2021 years, we can find IoT device breaches of over one billion, according to reports by Kaspersky, a major endpoint security solutions vendor [39],[41]. Moreover, most individuals are unaware of IoT devices and their inherent risks. Nevertheless, they also do not understand how serious the IoT security issues are.

Thus, it is important to understand the security challenges that systems face before understanding how to secure them when building systems. These challenges and threats must be addressed through a series of steps to eliminate or minimize them.

Volume: 14 Issue: 03 Pages: 5444-5454(2022) ISSN: 0975-0290

### *B. IoT Architecture and Security Challenges*

The introduction of IoT has become so popular in a very short time because it's a very simple and cheap platform that provides very good solutions to many problems and tasks that could not be done or solved. IoT has been used extensively in various fields, such as agriculture, manufacturing, military, etc. [54]-[59]. However, as they become more widely used, their risks and threats can be identified as a key challenge to IoT [14],[15].

In general, the IoT architecture can be apportioned into four layers: application layer, data processing (software) layer, network layer, and sensing (physical) layer, according to the research [2]-[7],[60]-[65]. According to this architecture, each layer operates under different technologies, whereas various challenges and vulnerabilities related to security have emerged pertained to each layer. Figure 1 specifies the different technologies, various devices, and applications used in each layer for better understanding.

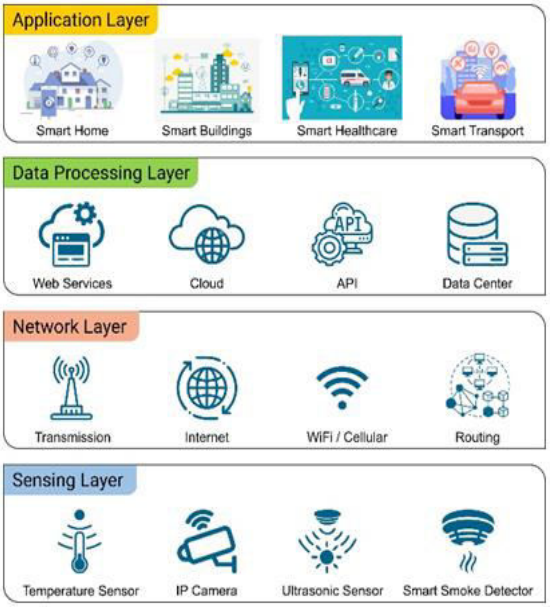


**Figure 1. IoT layered Architecture**

In the upcoming subsections, we briefly provide a overview on security attacks that target each layer.

### *C. Security challenges in the sensing layer*

The sensing layer is responsible for sensors and other hardware devices in IoT systems. Different types of sensors, such as smoke detectors, sensors in cameras, ultrasonic sensors, temperature sensors, etc., can be used to collect important data about the surroundings where they are placed [53],[54] at the sensing layer.

- ***Malicious code injection attack***
  In code injection attacks, the attacker uses malicious codes to execute attacks. This malicious code is then inserted into the memory of the physical nodes. As a result, attackers may force nodes to perform unnecessary operations or attempt to gain access to the IoT device [52].

- ***Fallacious data injection attack***
  The attacker first catches the node and injects fallacious or misleading data into its IoT, eventually malfunctioning IoT applications [65]-[68]. This method could also be used to launch a Denial of Service (DOS) attack.

- ***Node capturing***
  In node capturing, the attackers try to catch or replace an existing node with a malicious node. The new hostile node act as a part of the system, where the attacker can control the new malicious node, which severely impacts the security of the IoT system [56].

- ***Intervention and eavesdropping***
  IoT systems frequently contain several nodes deployed in an unsecured environment. In such cases, unauthorized users can use them to gain unauthorized access to the system if they are not secured enough [57]. Further, attackers can read and collect data over many processes, such as authentication or data transmission, and these attacks can lead to data leakage and unauthorized access to user data.

- ***Side-Channel attacks***
  In the side channel attack, sensitive data on the micro-architecture of the processors, power consumption, and electromagnetic emission can be revealed to the attacker. Examples of side-channel attacks are over-consumption of energy, electromagnetic attacks, timing attacks, and laser-based attacks. Many protections are included in modern CPUs to prevent side-channel attacks [52].

- ***Sleep deprivation attack***
  Attackers aim to drain IoT devices from this kind of attack. As IoT devices have a small battery capacity, they cannot produce enough power when the resources are highly utilized. As a result, the IoT system faces denial-of-service conditions, which would drain all its power [55].

- ***Booting attacks***
  Booting time is the most vulnerable period in any IoT device as the device manufacturers are designed to implement security features after booting time. As the features are not enabled at the booting time when node devices are rebooted, attackers may exploit this vulnerability and attempt to attack, compromising its security [68]-[72].

- ***Unknown device vendors***
  Most IoT-related sensors and devices are made by unknown Chinese vendors. They use customized operating systems and less secure

Volume: 14 Issue: 03 Pages: 5444-5454(2022) ISSN: 0975-0290

basic firmware for their hardware whereas these types of devices can't be trusted to handle our data securely. At times, they might implement some tracking tools to send our data secretly to their sources [16],[17].

- ***Low physical security of devices***
  When using an IoT platform for remote monitoring purposes, we use sensors to gather some data where they would be placed in public or outdoor locations. This always risks the devices as the security is not tight in these locations [17].
- ***Visible device debug ports***
  Debug ports of IoT devices are used to connect and analyze the device's log and error information [17]. These ports must be accessed only by authorized persons, whereas most device manufacturers designed IoT devices in such a way without providing adequate security for these external debug ports [20], [25].
- ***Unverified third-party components utilized in IoT devices***
  IoT devices commonly use third-party firmware, such as open-source libraries or chip components. Built-in security features and inherent security vulnerabilities of these third-party components would also be inherited by IoT upon the connection of these components with IoT [21], [25].
- ***Exploiting Universal Plug-and-Play (UPnP)***
  UPnP connects network-enabled devices instantly and seamlessly. For example, CCTV cameras use UPnP to communicate with routers and allow external connections to connect to local devices enabling consumers to connect their devices to the Internet easily. But it also opens connected devices to the rest of the world through Internet, which would pave the way for attackers to get inside users' devices through the UPnP protocol [27].

### *D. Security challenges in the network layer*

Transferring data from the sensing layer to the data processing layer is the major function of the network layer. The key security concerns at the network layer are listed below for better understanding.

- ***DoS attack***
  In this type of attack, the attacker makes a high number of unwanted requests to the target servers or the network device. As a result, the target server/network would be disabled, affecting all its user services. A Distributed Denial of Service (DDoS) attack occurs when an attacker combines many sources to overload the target server. Although such attacks are not unique to IoT applications, the network layer of the IoT is vulnerable to them due to the heterogeneity and complexity of the IoT networking infrastructure [60],[72]-[76].
- ***Routing attacks***
  In routing attacks, malicious nodes may try to divert information over the Internet. Sinkhole attacks are routing attacks in which an adversary shows a false shortest routing pathway and recruits network nodes to route traffic through it [58]. A wormhole attack is another routing attack that may be extremely dangerous when coupled with other types of attacks, such as sinkhole attacks [27]. By constructing a warm hole between a hacked node and a device on the Internet, an attacker can try to overcome the fundamental security procedures of an IoT system [60].
- ***Cellular network intercepting***
  As IoT platforms work with the Internet to get Internet access, IoT devices most commonly use Wi-Fi or cellular connection. Many IoT devices work on cellular connections instead of Wi-Fi, as in cellular networks, as devices not only get internet access but also can get SMS services and Call services. On the contrary, using a cellular connection is not a secure option as attackers in the vicinity can create a fake cell site and listen to consumers' conversations, read their text messages secretly, or directly breach the devices [21],[27].
- ***Brute-force attack***
  In the past, email accounts and PCs faced brute-forcing attacks, whereas nowadays, IoT devices are found everywhere, posing doubt about securing them against brute force attacks. In brute-force attacks, the attacker attempt to access a device through SSH or Telnet ports with a list of commonly used credentials or collected account credentials from data breaches [28].

### *E. Security challenges in the data processing layer*

The data processing layer serves as an intermediate layer between the application layer and network layer in the IoT systems. The data processing layer is often comprised of powerful computing and storage facilities. Persistent data storage, Artificial Processing (AI) units, queuing systems, and other components are included in the data processing layer to further process the data gathered at the sensing layer [73]-[77]. In the data processing layer, cloud security and database security are two key challenges stakeholders must be aware of.

- ***Cloud malware injection***
  By injecting cloud malware into the virtual machine, the attacker can take control of the cloud virtual machine. Later the attacker can access the service requests and capture sensitive data on the cloud virtual machine [78].

Volume: 14 Issue: 03 Pages: 5444-5454(2022) ISSN: 0975-0290

- ***SQL injection attack***
  In the SQL Injection (SQLi) attack, an attacker can include malicious SQL statements in service requests that are made to the cloud [62]. By doing so, an attacker can obtain sensitive information from the database and even insert data into database entries [63].
- ***Flooding attack in cloud***
  Flooding attack has an impact on quality of service (QoS). To drain cloud resources, attackers regularly send many requests to the cloud, which is the same as performing a cloud DoS attack. Therefore, by extending the load on cloud servers, these attacks can have a major effect on the availability of cloud servers.

### *F. Security Challenges at Application Layer*

End-users are directly interacted with and served by the application layer. This layer contains several security flaws, including data theft and privacy problems. Many IoT systems additionally have an application support layer between the network and application layers. It delivers various corporate services and assists in resource allocation and computation.

- ***Service interruption attacks***
  Commonly known as DDOS attacks or illegitimate interruption attacks. Here the attacker purposefully floods the network or servers with many requests. As a result, servers may become too busy to react, or services may become unavailable. Such attacks discourage legal consumers from using the services.
- ***Data theft***
  IoT systems often handle a massive amount of data. As IoT devices and platforms are always interconnected with the Internet, there is a high chance of intruders looking in to break into such devices seeking access to personal data. Personal information of the users, location coordinates, sensor readings, IP address, email, mobile phones, and CCTV camera data are all vulnerable to this data theft attacks. To secure IoT devices from data theft, technologies and protocols such as privacy management, user and network authentication, data isolation, and data encryption could be used [18],[24].
- ***Sniffing attacks***
  If there aren't adequate protective mechanisms in place to prevent sniffer attacks, attackers might use sniffer programs to monitor unwanted network traffic in IoT applications [70]-[75].
- ***Using default credentials***
  When consumers buy new IoT devices, the devices come with a default username and password set up by the device manufacturers. Recent research shows that default passwords are used by 15% of IoT devices which is a bad habit in consumers that will lead to losing the privacy of data stored in devices [23].
- ***Low-Level transport encryption***
  At times, IoT devices connected to the Internet use HTTP unencrypted protocols for intercommunication [15]. In such cases, devices share their credentials with other devices as plain text on an HTTP connection, where attackers on the network can easily view the data communicating on devices [22].

### *G. Real-World IoT Security Incidents*

- ***Nortek Security and Control: Access control system breach – 2019***
  Applied Risk (a cyber security firm) computer security service in Amsterdam discovered ten vulnerabilities in eMerge E3 in Nortek Linear devices in 2019. They found that hackers could steal credentials, take control of devices (opening/locking doors), install malware into the devices, and launch DoS (Denial of Service) attacks [73].
- ***Ring Home: Security camera breach – 2019***
  Ring Home is an Amazon-owned security camera solution provider that has built notoriety for itself in recent years due to two significant security issues. The first was due to an IoT security issue in which cybercriminals successfully hacked into multiple families' connected doorbells and home monitoring systems. The second was due to third-party trackers in their Android app mistakenly revealing user data to both Facebook and Google. Hackers could access live feeds from cameras surrounding users' houses and even engage remotely via the devices' integrated microphones and speakers using a combination of insecure and default credentials [72].
- ***The Hackable Cardiac Devices from St. Jude – 2017***
  In 2017 CNN reported that "St. Jude Medical's implantable cardiac" small IoT heart monitoring device is vulnerable and can be accessed by hackers. The device helps physicians monitor and manage patients' heart rates and prevents sudden heart attacks. The news also reported this device's wireless transmitter share patient heart condition status with physicians. To get control, hackers connect to the transmitter and have full control after that [27], [33].
- ***The Mirai Botnet – 2016***
  In 2016 a large DDoS attack happened, suffering a number of major websites worldwide, including the world's most famous websites such as Reddit, Netflix, Guardian, Twitter, and CNN. This has happened owing to an IoT botnet called Mirai [26], [32].

Volume: 14 Issue: 03 Pages: 5444-5454(2022) ISSN: 0975-0290

## III. ENSURING THE SECURITY OF IOT SYSTEMS: WHAT MUST BE DONE?

Unsecured IoT devices can allow attackers access to networks and other linked devices [76]-[80]. As IoT devices have a wide attack surface and a large supply of security faults, cybercriminals frequently target them in cyber-attacks [80]-[84]. As the number of linked devices increases, ensuring IoT security without the necessary knowledge and methods becomes increasingly difficult. Hence in the following, we provide a brief overview of what measures can be taken to improve the security of IoT systems.

- ***Authentication and authorization***
  To limit or decrease network vulnerabilities and breaches, IoT applications must implement authentication services such as access control methods. Improper device authentication allows attackers to direct access, creating a security risk [44],[47]. Access control, however, limits the privileges of IoT device components and applications. It defines who has been permitted access to the data and IoT devices and how much access they should be given. And it ensures that data is only accessible to authorized users and utilizes strong authentication to authorize them. So, they get access only to the resources they need.
  Further, it is also necessary to apply a strong password, fingerprint or facial identity, or other biometric authentication means to verify the user's identity; to allow access to the user data [44]. Password protection must be strong to avoid brute force attacks [47]. When configuring the password, the user should ensure that each IoT device has different passwords, change passwords at least several times a year, and avoid common and general passwords [46]. On the other hand, for IoT devices to ensure maximum security and privacy, well-structured access control must be required [45].

- ***Data encryption and integrity***
  All sensitive data must be encrypted during the data storage or transmission phase [47]. Even if attackers gain access to the transmission media or database, well-built data encryption makes it tough for them to access sensitive user data [45].

- ***Data minimization***
  This is the best practice for maintaining a safe data repository within an organization by minimizing the duration of the repository. As a privacy measure, it suggests that IoT services should minimize gathering personal data by only collecting needed data [48]. An organization should obtain data for a specific period and delete unwanted personal user data that is no longer needed. Too much gathering of personal data and maintaining a large data repository can have a lot of potential for security breaches.

- ***Continuous monitoring and reporting***
  IoT devices should monitor regular and continual data collection as a preventative measure against cyber-attacks [44]. In a centralized log management system, all IoT applications and device-related logs must be collected, whereby implementing a centralized system can monitor and analyze network and internet attacks continuously.

- ***Manage updates of devices***
  A lack of device updates is one of the biggest IoT security issues [46]. Automatic updates must be in place in IoT devices to check for official updates by the device manufacturer. IoT manufacturers often release security patches every quarter [44]. Operating system versions and security patches are also upgraded as part of these updates. When working with users' IoT device makers, they need to develop patch management and firmware upgrade plan. Also, it's vital to ensure users' devices are updated to the latest version. This ensures that the system's security is up to date, and the system's data must be safeguarded in all aspects [47].

- ***Minimize device bandwidth***
  Limiting the amount of network traffic essential for the IoT devices to function. If possible, configure the devices to restrict hardware and kernel-level bandwidth while observing suspicious activities. This will protect IoT systems against Denial-of-Service attacks.

- ***Using Honeypots***
  The most popular method of securing IoT is using honeypots. These decoy programs appear reliable but are specifically developed to catch attackers attempting to attack a system. The attackers are stealthily watched throughout the process without the intruder's knowledge. The honeypot information can be transferred to a sandbox for automated analysis. This enables us to anticipate attacks, gather and analyze malware targeting IoT devices, and respond quickly to remediation operations [76].

- ***Follow best practices***
  Implementing firewalls, lightweight encryption, hardening, and eliminating device backdoor channels are all strategies to secure the IoT system from harm. Because these IoT devices and apps are always linked to the Internet, network security should be ensured by implementing hypertext transfer protocol secure (HTTPS), intrusion prevention systems (IPSs), security sockets layer (SSL)/transport security layer (TSL), and intrusion detection systems (IDSs) [45]. On the other hand, before installing an IoT device, a risk management assessment should be carried out to identify any potential

Volume: 14 Issue: 03 Pages: 5444-5454(2022) ISSN: 0975-0290

vulnerabilities before setting up the system environment [49].

## IV. FUTURE DIRECTIONS OF THE IOT SECURITY CHALLENGES

Our lives will be made easier when the network capabilities are expanded to all possible physical locations, but the growth of IoT will raise the number of potential threats, which will influence device productivity and safety [85]-[90]. With the development of the IoT, various technologies will emerge that can make the next generation of IoT more secure. This section intends to provide users with a summary of the anticipated future directions regarding IoT security.

- ***Blockchain and IoT security***
  Blockchain technology became well-known with the emergence of cryptocurrency mining, and currently, the technology is used for designing robust, secure systems. The data processed by IoT devices is vast and always vulnerable to cyber-attacks. Thus, it's possible to use blockchain to standardize, authenticate, and safeguard the adoption of data handled by such devices. In general, blockchain can keep track of the data collected using sensors without allowing it to be replicated by erroneous data. Further, blockchain technology provides security to; data collected in real-time from IoT sensors by storing this data in blockchain ledgers [78].

- ***IoT Security and Fogcomputing***
  IoT devices produce massive amounts of data regularly, and it is not easy to manage and move the generated data to the cloud storage for analysis in real time. As a solution, the Fog computing concept has been developed where cloud computing services are being extended to the network's edge by Fog Computing. It aims to improve security, avoid data theft, decrease the quantity of data saved in the cloud, and improve the overall efficiency of IoT devices. [81].

- ***IoT security and Edge computing***
  An edge computing: system's compute and analytical capacity is delivered right at the network edge. The devices in an application can form a network and collaborate to compute data. As a result, a considerable amount of data can be prevented from being sent outside the device, either to the cloud or to fog nodes. So, the security of IoT applications can be improved. Edge computing also helps to reduce transmission costs by eliminating the need to send all data to the cloud [52].

- ***IoT security and AI***
  There has been much interest in AI with IoT in recent years. Many fields are emerging with AI and are also being used to secure IoT devices. As AI introduces various approaches to securing networks against real-time threats, it seems to be a good preventive method to protect IoT devices against cyber threats [90],[91]. The security of all devices connected to the network is an important requirement of IoT. In such cases, the role of AI is to develop and train algorithms for detecting anomalies in IoT devices or any undesired activity occurring in an IoT system, to secure data loss or other difficulties. As a result, machine learning and deep learning provide a potential foundation for solving the issues of protecting IoT devices [82].

- ***Cryptographic techniques***
  - ✓ *Homographic encryption*
    Homomorphic Encryption (HE) is a unique encryption technology that enables computations on encrypted data without demanding access to a secret (decryption) key. The computations' outcomes are encrypted, and only the secret key holder can reveal that data [79].
  - ✓ *Searchable encryption*
    Searchable Encryption (SE) is a cryptographic mechanism that enables secure searching of encrypted data. This allows a human or an automated program to execute a safe query for a particular incident without jeopardizing the confidentiality of data [80].

  Future IoT systems will use these technologies to respond rapidly and properly to threats and attacks, learn and incorporate new threat information, and design and implement threat mitigation actions. They will also be able to ensure that data ownership is controlled across business boundaries. In the future, new data analytics algorithms and encryption approaches will be applied to secure the privacy of users and organizations while processing massive amounts of data. Risk assessment and risk management methods such as threat analytics algorithms would be introduced using the above technologies. As a result, in the future, organizations and device manufacturers will assess the effect of vulnerabilities and design particular control mechanisms through constant testing & evaluation.

## V. CONCLUSION

In this research, we have reviewed the latest status of IoT security, highlighting challenges and countermeasures. In this regard, we have summarized different security challenges that persist at the different layers of the IoT architecture, namely at the application layer, data processing layer, network layer, and physical layer. We have identified all these challenges and highlighted what countermeasures can be taken to protect from these

Volume: 14 Issue: 03 Pages: 5444-5454(2022) ISSN: 0975-0290

security challenges. We believe this research will help select secure IoT technologies for an organization and would be a worthwhile resource for security enhancement for future IoT applications.

## REFERENCES


[1] Vailshery, L., 2022. Global IoT and non-IoT connections 2010-2025 | Statista. [online] Statista. Available: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/#:~:text=The%20total%20installed%20base%20of,that%20are%20expected%20in%202021.

[2] IOT - google trends. (n.d.). Available: https://trends.google.com/trends/explore?date=all&q=iot.

[3] Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine learning in IOT security: Current solutions and future challenges. IEEE Communications Surveys & Tutorials, 22(3), 1686–1721.

[4] Thilakarathne, N. N., Weerasinghe, H. D., Welhenge, A., & Kagita, M. K. (2021). Privacy dilemma in healthcare: A review on Privacy Preserving Medical Internet of Things. 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT).

[5] Alhalafi, N., & Veeraraghavan, P. (2019). Privacy and security challenges and solutions in IOT: A Review. IOP Conference Series: Earth and Environmental Science, 322(1), 012013.

[6] History of I.O.T. Trinity. (2021, July 4). Available: https://www.trinity.co.za/docs/history-of-iot/.

[7] The history of IOT security. History in the Making. Available: https://publications.psacertified.org/the-history-of-iot-security/history-in-the-making/.

[8] Suresh, P., Daniel, J. V., Parthasarathy, V., & Aswathy, R. H. (2014). A state of the art review on the Internet of things (IOT) history, technology and fields of deployment. 2014 International Conference on Science Engineering and Management Research (ICSEMR).

[9] Internet of things (IOT) history. Postscapes. (2019, November 12). Available: https://www.postscapes.com/iot-history/.

[10] Ashton, K. (2020, July 1). That 'Internet of things' thing. RFID JOURNAL. Available: http://www.rfidjournal.com/articles/view?4986.

[11] Gloukhovtsev, M. (2018). IOT security: Challenges, Solutions & Future prospects - dell emc. Available: https://education.dellemc.com/content/dam/dell-emc/documents/en-us/2018KS_Gloukhovtsev-IoT_Security_Challenges_Solutions_and_Future_Prospects.pdf.

[12] Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S., & Mustaqim, M. (2020). Internet of things (IOT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IOT scenarios. IEEE Access, 8, 23022–23040

[13] Cyber Hub. (2022, March 8). IOT security issues. Check Point Software. Available: https://www.checkpoint.com/cyber-hub/network-security/what-is-iot-security/iot-security-issues/.

[14] "Security challenges of IOT-Enabled Solutions: ISACA Journal," ISACA [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-4/security-and-privacy-challenges-of-iot-enabled-solutions.

[15] Security Innovation Follow, "Security Testing for IOT Systems," SlideShare a Scribd company. [Online]. Available: https://www.slideshare.net/SecurityInnovation/security-testing-for-iot-systems?next_slideshow=149455670.

[16] YashKesharwani2 Follow, "IOT security," SlideShare a Scribd company. [Online]. Available: https://www.slideshare.net/YashKesharwani2/iot-security-113025045.

[17] Somasundaram Jambunathan Follow Associate Director at Cognizant Technology Solutions, "Security and privacy considerations in internet of things," SlideShare a Scribd company. [Online]. Available: https://www.slideshare.net/somaj/security-and-privacy-considerations-in-internet-of-things-45331113.

[18] Radouane Mrabet Follow Président, "IOT security and privacy: Main challenges and how ISOC-Ota Address Th...," SlideShare a Scribd company. [Online]. Available: https://www.slideshare.net/RadouaneMrabet/iot-security-and-privacy-main-challenges-and-how-isocota-address-them.

[19] Emertxe Information Technologies Pvt Ltd Follow, "Design challenges in IOT," SlideShare a Scribd company. [Online]. Available: https://www.slideshare.net/EmertxeSlides/design-challenges-iotemertxev20?qid=c11b1607-5c74-4bcd-87e4-778fdf2cc7a0&v=&b=&from_search=2.

[20] J. Borgini, "Top advantages and disadvantages of IOT in business," IoT Agenda, 29-Mar-2022. [Online]. Available: https://www.techtarget.com/iotagenda/tip/Top-advantages-and-disadvantages-of-IoT-in-business.

[21] Charalampos Doukas Follow Senior Researcher at CREATE-NET, "Hardware challenges for the IOT," SlideShare a Scribd company. [Online]. Available: https://www.slideshare.net/CharalamposDoukas/hardware-challenges-for-the-iot?qid=d0841cea-e2f7-4b40-8e46-31091a69737d&v=&b=&from_search=2.

[22] Koenig Solutions Ltd. Follow IT Training Institute, "IOT security, threats and challenges by V.P.Prabhakaran," SlideShare a Scribd company. [Online]. Available: https://www.slideshare.net/KoenigSolutionsLtd/iot-security-threats-and-challenges-by-by-vpprabhakaran?qid=926ab273-5a17-4a51-bf9a-11e916ada512&v=&b=&from_search=4.

[23] E. Yang, "15% of IOT devices use default passwords: Research," The comprehensive security industry

Volume: 14 Issue: 03 Pages: 5444-5454(2022) ISSN: 0975-0290

platform, 21-Jun-2017. [Online]. Available: https://www.asmag.com/showpost/26498.aspx.

[24] "17 biggest security challenges for IOT," Peerbits, 07-Apr-2022. [Online]. Available: https://www.peerbits.com/blog/biggest-iot-security-challenges.html.

[25] "Top 11 IOT cybersecurity challenges facing businesses," SecurityScorecard. [Online]. Available: https://securityscorecard.com/blog/top-iot-cybersecurity-challenges-facing-businesses.

[26] T. D.-J. 20, "The 5 worst examples of IOT hacking and vulnerabilities in recorded history," IoT For All, 28-Mar-2022. [Online]. Available: https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities.

[27] "4 ways cyber attackers may be hacking your IOT devices right now," Operator by Hologram. [Online]. Available: https://www.hologram.io/blog/4-ways-cyber-attackers-may-be-hacking-your-iot-devices-right-now.

[28] N. Kovartovsky, "Brute force attacks on IOT - here to stay?: Allot blog," ALLOT, 22-Mar-2022. [Online]. Available: https://www.allot.com/blog/brute-force-attacks-iot/#:~:text=Recent%20IoT%20Attacks%3A&text=At%20the%20root%20of%20Mirai,hidden%20and%20default%20account%20credentials.

[29] M. Noura, M. Atiquzzaman, and M. Gaedke, "Interoperability in internet of things: Taxonomies and open challenges - mobile networks and applications," SpringerLink, 21-Jul-2018. [Online]. Available: https://link.springer.com/article/10.1007/s11036-018-1089-9.

[30] "A survey in Hello Flood attack in wireless sensor networks - I. JERT" [Online]. Available: https://www.ijert.org/research/a-survey-in-hello-flood-attack-in-wireless-sensor-networks-IJERTV3IS10747.pdf.

[31] "Top 4 challenges in IOT data collection and management," FirstPoint, 25-Oct-2021. [Online]. Available: https://www.firstpoint-mg.com/blog/top-4-challenges-in-iot-data-collection-and-management/.

[32] "Mirai botnet: Three admit creating and Running Attack Tool," BBC News, 13-Dec-2017. [Online]. Available: https://www.bbc.com/news/technology-42342221.

[33] The FDA confirmed that St. Jude Medical's implantable cardiac devices have vulnerabilities that could allow a hacker to access a device. Once in, "FDA confirms that St. Jude's cardiac devices can be hacked," CNNMoney. [Online]. Available: https://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack/.

[34] I. Thomson, "Wi-Fi Baby Heart Monitor may have the worst IOT security of 2016," The Register® - Biting the hand that feeds IT, 14-Oct-2016. [Online]. Available: https://www.theregister.com/2016/10/13/possibly_worst_iot_security_failure_yet/.

[35] L. Kelion, "Trendnet Security cam flaw exposes video feeds on NET," BBC News, 08-Mar-2012. [Online]. Available: https://www.bbc.com/news/technology-16919664.

[36] A. Drozhzhin, Y. Ilyin, L. Grustniy, A. Starikova, and H. Aver, "Black Hat USA 2015: The full story of how that Jeep was hacked," Daily English Global blogkasperskycom. [Online]. Available: https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/.

[37] S. Millar, "IOT security challenges and mitigations: An introduction - arxiv," 29-Dec-2021. [Online]. Available: https://arxiv.org/pdf/2112.14618.pdf.

[38] "Lecture 8: IOT security," YouTube, 26-Oct-2017. [Online]. Available: https://www.youtube.com/watch?v=4YAsAdCa9sU.

[39] B. Len Follow Webmaster., "IOT security, internet of things," SlideShare a Scribd company, 10-Jun-2020. [Online]. Available: https://www.slideshare.net/BryanLen1/iot-security-internet-of-things.

[40] E. -Msft, "Internet of things (IOT) security best practices," Internet of Things (IoT) security best practices | Microsoft Docs, 16-Nov-2021. [Online]. Available: https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices.

[41] A. Katrenko and E. Semeniak, "Internet of things (IOT) security: Challenges and best practices," Apriorit, 17-Feb-2022. [Online]. Available: https://www.apriorit.com/dev-blog/513-iot-security.

[42] R. van Kranenburg and A. Bassi, "(PDF) iot challenges - researchgate," (PDF) IoT Challenges, 2012. [Online]. Available: https://www.researchgate.net/publication/257885103_IoT_Challenges

[43] Liu, X.; Zhao, M.; Li, S.; Zhang, F.; Trappe, W. A security framework for the Internet of things in the future internet architecture. Future Internet 2017, 9, 27. [Google Scholar] [CrossRef].

[44] Tawalbeh, Lo'ai, Fadi Muheidat, Mais Tawalbeh, and Muhannad Quwaider. 2020. "IoT Privacy and Security: Challenges and Solutions" Applied Sciences 10, no. 12: 4102.

[45] Elhoseny, M., Thilakarathne, N. N., Alghamdi, M. I., Mahendran, R. K., Gardezi, A. A., Weerasinghe, H., & Welhenge, A. (2021, October 21). Security and privacy issues in medical Internet of things: Overview, countermeasures, challenges and future directions. MDPI. Retrieved June 8, 2022, from https://www.mdpi.com/2071-1050/13/21/11645/htm.

[46] Design Rush. (2022, January 11). 7 IOT security issues and how to protect your solution. DesignRush. Retrieved June 8, 2022, from :https://www.designrush.com/agency/software-development/trends/iot-security-issues.

[47] CD-Team. (2017, April 14). IOT security – challenges and solutions: Internet of things. Electronics For You. Retrieved June 6, 2022, from https://www.electronicsforu.com/technology-trends/iot-security-challenges-solutions/2.

Volume: 14 Issue: 03 Pages: 5444-5454(2022) ISSN: 0975-0290

[48] Aldowah, Hanan & Rehman, Shafiq & Umar, Irfan. (2019). Security in Internet of Things: Issues, Challenges, and Solutions. 10.1007/978-3-319-99007-1_38.

[49] Kumar, Sathish & Vealey, Tyler & Srivastava, Harshit. (2016). Security in Internet of Things: Challenges, Solutions and Future Directions. 5772-5781. 10.1109/HICSS.2016.714.

[50] "Welcome to Engineers Australia Portal." Portal.engineersaustralia.org.au, portal.engineersaustralia.org.au/news/internet-things-poses-security-concerns.

[51] admin. "Man-In-The-Middle Attacks in the IoT." GlobalSign GMO Internet, Inc., 6 Feb. 2020, www.globalsign.com/en/blog/man-in-the-middle-attacks-iot.

[52] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IOT security: Application areas, security threats, and solution architectures. IEEE Access, 7, 82721–82743.

[53] Bridgera. "IoT System | Sensors and Actuators Overview - Bridgera." Bridgera, 24 Sept. 2018, bridgera.com/iot-system-sensors-actuators/.

[54] Smarthomeblog. How to Make Your Smoke Detecter Smarter. Available: https://www.smarthomeblog.net/smartsmoke-detector/

[55] Tictecbell. Sensor d'Ultrasons. [Online]. Available: https://sites.google.com/site/tictecbell/Arduino/ultrasons/

[56] S. Kumar, S. Sahoo, A. Mahapatra, A. K. Swain, and K. K. Mahapatra, ''Security enhancements to system on chip devices for IoT perception layer,'' in Proc. IEEE Int. Symp. Nanoelectron. Inf. Syst. (iNIS), 2017, pp. 151–156

[57] C.-H. Liao, H.-H. Shuai, and L.-C. Wang, ''Eavesdropping prevention for heterogeneous Internet of Things systems,'' in Proc. 15th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC), Jan. 2018, pp. 1–2.

[58] APWG Phishing Activity Trends Report. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q4_2017.pdf.

[59] C. Li and C. Chen, ''A multi-stage control method application in the fight against phishing attacks,'' in Proc. 26th Comput. Secur. Acad. Commun. Across Country, 2011, p. 145.

[60] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, ''DDoS in the IoT: Mirai and other Botnets,'' Computer, vol. 50, no. 7, pp. 80–84, 2017.

[61] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, ''A survey of middleware for Internet of Things,'' in Recent Trends in Wireless and Mobile Networks. Springer, 2011, pp. 288–296.

[62] Q. Zhang and X. Wang, ''SQL injections through back-end of RFID system,'' in Proc. Int. Symp. Comput. Netw. Multimedia Technol., Jan. 2009, pp. 1–4.

[63] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, ''Middleware for Internet of Things: A survey,'' IEEE Internet Things J., vol. 3, no. 1, pp. 70–95, Feb. 2016.

[64] Acunetix. Insecure Deserialization. [Online]. Available: https://www.acunetix.com/blog/articles/owasp-top-10-2017/

[65] J. Kumar, B. Rajendran, B. S. Bindhumadhava, and N. S. C. Babu, ''XML wrapping attack mitigation using positional token,'' in Proc. Int. Conf. Public Key Infrastruct. Appl. (PKIA), Nov. 2017, pp. 36–42.

[66] WS-Attacks. Attack Subtypes. [Online]. Available: https://www.ws-attacks.org/XML_Signature_Wrapping

[67] C. Fife. Securing the IoT Gateway. [Online]. Available: https://www.citrix.com/blogs/2015/07/24/securing-the-IoTgateway/.

[68] A. Stanciu, T.-C. Balan, C. Gerigan, and S. Zamfir, ''Securing the IoT gateway based on the hardware implementation of a multi pattern search algorithm,'' in Proc. Int. Conf. Optim. Elect. Electron. Equip. (OPTIM) Int. Aegean Conf. Elect. Mach. Power Electron. (ACEMP), May 2017, pp. 1001–1006.

[69] S.-C. Cha, J.-F. Chen, C. Su, and K.-H. Yeh, ''A blockchain connected gateway for BLE-based devices in the Internet of Things,'' IEEE Access, vol. 6, pp. 24639–24649, 2018.

[70] S. N. Swamy, D. Jadhav, and N. Kulkarni, ''Security threats in the application layer in IoT applications,'' in Proc. Int. Conf. IoT Social, Mobile, Analytics Cloud (I-SMAC), 477–480.

[71] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, ''A comprehensive IoT attacks survey based on a building-blocked reference model,'' Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 3, pp. 355–373, 2018.

[72] "Ring Hacked: How to Protect Your Ring Smart Device | NordVPN." Nordvpn.com, 23 Dec. 2021, nordvpn.com/blog/ring-doorbell-hack/#:~:text=In%202019%2C%20more%20than%203000.

[73] "IoT Security Breaches: 4 Real-World Examples." Conosco, 28 Jan. 2021, www.conosco.com/blog/iot-security-breaches-4-real-world-examples/#:~:text=In%20fact%2C%2084%25%20of%20surveyed. Accessed 8 June 2022.

[74] Eross-Msft, "IOT security architecture," IoT Security Architecture | Microsoft Docs, 30-Nov-2021. [Online]. Available: https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture.

[75] B. Witten, "Internet of things (IOT) cornerstones of security - ppt download," SlidePlayer, 25-Jun-2015. [Online]. Available: https://slideplayer.com/slide/6216442/.

[76] R, Ranjisha, and Sowmya S Gowda. IOT SECURITY: CHALLENGES and FUTURE TRENDS. Dell Technologies, 1 Jan. 2021, education.dellemc.com/content/dam/dell-emc/documents/en-us/2021KS_Ranjisha-IOT_Security_Challenges_and_Future_Trends.pdf.

Volume: 14 Issue: 03 Pages: 5444-5454(2022) ISSN: 0975-0290

[77] Thilakarathne, N. N., Muneeswari, G., Parthasarathy, V., Alassery, F., Hamam, H., Mahendran, R. K., & Shafiq, M. (2022). Federated Learning for Privacy-Preserved Medical Internet of Things. INTELLIGENT AUTOMATION AND SOFT COMPUTING, 33(1), 157-172.

[78] "Blockchain and IoT Security: Everything You Need to Know." Chakray, 26 Feb. 2019, www.chakray.com/blockchain-iot-security/#:~:text=For%20IoT%20safety%2C%20the%20blockchain.

[79] D. Miller, ''Blockchain and the Internet of Things in the industrial sector,'' IT Prof., vol. 20, no. 3, pp. 15–18, 2018.

[80] Thilakarathne, N. N., & Madhuka Priyashan, W. D. (2022). An Overview of Security and Privacy in Smart Cities. IoT and IoE Driven Smart Cities, 21-44.

[81] "What Is Homomorphic Encryption, and Why Isn't It Mainstream?" Keyfactor, www.keyfactor.com/blog/what-is-homomorphic-encryption/.

[82] Chamili, Khadijah, et al. "Searchable Encryption: A Review." International Journal of Security and Its Applications, vol. 11, no. 12, 31 Dec. 2017, pp. 79–88, article.nadiapub.com/IJSIA/vol11_no12/7.pdf, 10.14257/ijsia.2017.11.12.07. Accessed 3 Mar. 2022.

[83] Thilakarathne, N. N., Weerawarna, N. T., & Mahendran, R. K. (2021). Cyber Attacks Evaluation Targeting Internet Facing IoT: An Experimental Evaluation. Journal of Cybersecurity and Information Management (JCIM) Vol, 9(1), 18-26.

[84] Alrawais, Arwa, et al. "Fog Computing for the Internet of Things: Security and Privacy Issues." IEEE Internet Computing, vol. 21, no. 2, Mar. 2017, pp. 34–42, 10.1109/mic.2017.37.

[85] Ahmad, Rasheed, and Izzat Alsmadi. "Machine Learning Approaches to IoT Security: A Systematic Literature Review." Internet of Things, Jan. 2021, p. 100365, 10.1016/j.iot.2021.100365.

[86] Ankergård, Sigurd Frej Joel Jørgensen, et al. "State-of-The-Art Software-Based Remote Attestation: Opportunities and Open Issues for Internet of Things." Sensors, vol. 21, no. 5, 25 Feb. 2021, p. 1598, 10.3390/s21051598.

[87] Thilakarathne, N. N. (2020). Security and privacy issues in iot environment. International Journal of Engineering and Management Research, 10.

[88] Thilakarathne, N. N., & Wickramaaarachchi, D. (2020). Improved hierarchical role based access control model for cloud computing. arXiv preprint arXiv:2011.07764.

[89] Bader, Jawhara, and Anna Lito Michala. "Searchable Encryption with Access Control in Industrial Internet of Things (IIoT)." Wireless Communications and Mobile Computing, vol. 2021, 15 May 2021, pp. 1–10, 10.1155/2021/5555362.

[90] Neranjan Thilakrathne, N., Samarasinghe, R., & Priyashan, M. (2021). Evaluation of Cyber Attacks Targeting Internet Facing IoT: An Experimental Evaluation. arXiv e-prints, arXiv-2201.