EAI Endorsed Transactions
on Internet of Things

Research Article **EAI.EU**

Fortifying the Internet of Things: A Comprehensive Security Review

Oroos Arshi[1], Aryan Chaudhary[2]

[1] 1Department of Cyber Security and Forensics, School of Computer Science, University of Petroleum and Energy Studies, Dehradun
2 Chief Scientific Advisor, Bio Tech Sphere Research, India

Abstract

A variety of new technologies and their related capabilities have entered daily life in the long run of IoT technology. Various industrial sectors, including healthcare, facility management, agriculture, energy, and transportation, use IoT technologies. Interconnected networks are starting to include IoT devices like wearables, commercial appliances, connected electronics, smart grids, smart automobiles, etc. These gadgets produce enormous amounts of data, which are gathered, examined, recorded, and kept on the networks. IoT security is challenging to secure since the devices employ basic processors and operating systems that may not be compatible with advanced security measures. The information and the devices that are used by organizations as a part of their network must be protected against hackers. In this paper, we discuss the overall review of IoT systems that contain the scope of IoT in the future era, some of the characteristics of IoT systems, and layers including the working Architecture of IoT. We will also discuss some of the vulnerabilities surface area attacks, and application areas regarding IoT. Potential weaknesses in the IoT system could cause serious issues for enterprises. The majority of Internet of Things (IoT) devices have security flaws, including incorrect physical security systems, lack of lock-out mechanisms, weak encryption schemes, improper key management systems, improper authentication mechanisms, the use of default credentials, Intrusion detection systems using Graph Neural network and drawbacks of existing IoT security Challenges. As in the evolving era, security issues are becoming a major problem so some of the security threats of IoT are also mentioned here. This paper also provides the methods for addressing the vulnerabilities of IoT systems.

Keywords: IoT security, Intrusion detection System, Graph neural Networks, Internet-of-things (IoT), Security threats

Received on 25 July 2023, accepted on 26 September 2023, published on 02 October 2023

doi: 10.4108/eetiot.v9i4.3618

*Corresponding author. Email: chaudhary.aryan@biotechsphereresearch.com

1. Introduction

The term "Internet of Things" (IoT) or "Internet of Everything" (IoE) involves a system of IP-enabled devices which can sense, gather, and communicate data using embedded sensors, communication hardware, and processors [1]. In the Internet of Things, an object is referred to as a thing if it has a device installed on it that is capable of communicating through a network with other natural, artificial, or machine-made objects. IoT is used because it gives users complete control over their life and enables them to live and work more intelligently. . IoT is crucial to business and offers intelligent home automation gadgets. With real-time insights into how systems actually function, provided by IoT, businesses can better understand all aspects of equipment performance, production lines, and logistics activities. Among the most important technological advancements in modern existence is the Internet of Things (IoT), and it will gain momentum as more companies discover how competitively advantageous connected gadgets can be [2]. A wide range of prospects for improving company and consumer satisfaction are made possible by the development in networking capabilities of machines and commonplace appliances used in several sectors, including workplaces, residences, industries, transportation, construction, and wearable gadgets. Connectivity, sensors, artificial intelligence, small devices, and active involvement few of the most crucial elements of the Internet of Things [3].

This is how the paper is structured:
An overview of the internet of things is provided in Section 1. IoT security-related works are presented in Section 2 of this article. the Internet of Things framework is presented in section 3. Section 4 describes IoT protocol and technologies. The function of the operating system in IoT devices is demonstrated in Section 5. Section 6 discusses the concerns for managing IoT device attack surfaces, and Section 7 discusses the security threat in an IoT ecosystem and also provide IoT system vulnerabilities in software in section 8 are discussed, along with potential fixes in Section 9 is discussed, IoT application areas are covered in section 10, Challenges and Drawbacks of Existing IoT Security Approaches in shown in section 11, Proposed approaches in IoT security Enhancement is disused in section 12, Graph neural networks (GNNs) in IoT security , Enhancing Intrusion detection with Graph Neural network (GNNs) is discussed in section 13 and conclusion in section 14.

1.1 Understanding the Mechanism of IoT: How the Internet of things works

IoT technology consists of three main systems: IoT devices, gateway systems, data storage systems that use the cloud, and mobile apps for remote control. The communication between two end points is made possible by these systems working together. Here Figure 1 explains the working of IoT systems. Several essential IoT technology elements that are crucial to the operation of an IoT device are mentioned below:

(a) **Sensing technology:** The gadgets have sensors built into them that detect a variety of information about their environment, including gases, temperature, location, the operation of various industrial machinery, and patient health information.

(b) **IoT gateways:** Gateways serves as to connect and communicate involving the IoT device and the user by bridging the distance between them. IoT devices use sensors to gather data, which is then sent to the cloud or to the concerned user through a gateway**.**

(c) **Cloud server/ data storage:** After passing via the gateway, the collected data is received to the cloud, where it is saved and put through data analysis. The user then obtains the processed data and uses it to make decisions on the basis on the information that has been provided to him or her.

(d) **Mobile app remote control:** The consumer may monitor, manage, retrieve data from, and perform particular actions on IoT devices from a distance using mobile phones and remote controls, laptops and tablets etc, that have a mobile app installed to them.

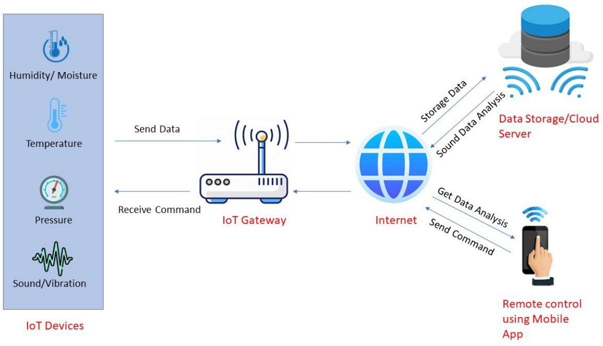

Fig 1. Working of IoT system

Example:

1. The gateway, which aids in connecting the gadget to the internet and the cloud infrastructure, will be connected to the smart security system placed in a home.

2. Every device linked to the network is represented in the data storage in the cloud. The data held contains the device's id, its current condition, a list of all users who have accessed the device, and information on how frequently they did so. It also contains details like the most recent duration of access to the device.

3. Web services are used to establish the connection with the cloud server.

4. The user on the other side, who has the necessary app to remotely access the gadget on his mobile phone, engages with it, which in turn causes him to engage with the devices at home. He is required to authenticate himself before being granted access to the device, and if his credentials match those stored in the cloud, he is allowed access. Otherwise, access is restricted to him to maintain security. The cloud server uses gateways to

   recognize the device's id and make a request specific to it.

5. When a security system that is currently capturing video at a home detects any strange activity, it sends a warning to the cloud through a gateway, which matches the device's id with the user who is associated with it, and then sends a warning to the end user.

1.2 Key characteristics of Internet of things (IoT)

Figure 2 shows some characteristics of IoT system. Let's talk about them one by one [4][5].

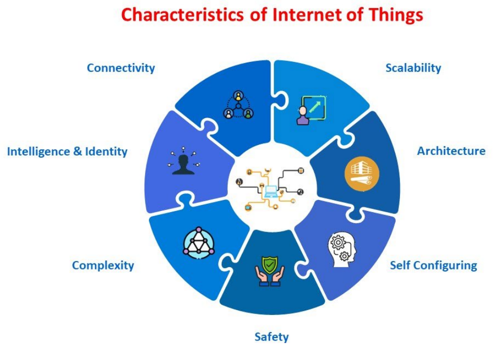

Figure 2. Characteristics of IOT system

1. Connectivity- The communication of the IoT infrastructure is a crucial element. It is essential to connect IoT devices to IoT infrastructure. It should always be accessible for anybody, everywhere, to connect. Consider connections between users of internet-capable such as smartphones and other technology, along with connections between world wide web devices like routers, gateways, sensors, etc**.** [4][5].

2. Scalability- The Internet of Things is being broadened regularly to include more and more gadgets. IoT platforms must therefore be capable of handling the massive development. Because of the huge amount of information generated, it has to be managed appropriately. [4][5].

3. Intelligence and Identity - It's crucial to retrieve knowledge based on the information that is produced. When a sensor, for instance, creates data, it must be properly processed for the data to be useful. There is a distinct identification for every IoT device. This identity helps trace the device and periodically check on its condition. [4][5].

4. Architecture- The IoT architecture is not uniform by nature. For the IoT network to function, it should be hybrid and support goods from many manufacturers. The engineering branch does not own the Internet of Things. When several fields come together, IoT becomes a reality [4][5].

5. Self-Adaptive and Dynamic (Complexity)- IoT systems should be able to adapt to a variety of scenarios and circumstances on the go. Assume there is a camera for surveillance. It should have the versatility to work in a variety of lighting and environmental factors (night, afternoon, and morning) [4][5].

6. Self-configuring- The capacity of IoT to self-configure is some of the most crucial characteristics. The software on IoT devices can be updated to meet requirements with the least amount of user involvement. They can also set up the network, enabling the integration of new devices into an existing network [4][5].

7. Safety- Sensitive personal information may be jeopardised when a user's devices are all connected to the internet. As a result, the user can sustain a loss. Therefore, the primary problem is data protection. The required equipment is also very large. IoT networks may also be at risk. Device security is therefore crucial. [6][7].

2. Related Works

The IoT systems are a very advanced technology for the future, but as it expands, it is also encountering several security-related problems. Because of this, the majority of surveys and review articles are concentrating on security concerns and IoT countermeasures. Noor et al. [1] This paper looks at the developments and open issues in current Internet of Things security study during 2016 to 2018. This study's main goal is to provide an overview of the current state of safety for the internet of Things studies, including relevant tools, IoT modellers, and simulations. Zhang et al. [3] examines the history of information security for the Internet of Things as well as prospective problems that could arise in the future. The security issues the Internet of Things faces are also covered in this article along with possible research avenues. Gou et.al [6] examines the perceptions, network, and use-case strata of the IoT system to evaluate the IoT security issue. It then suggests a secure IoT architecture and offers corresponding secure remedies depending on the framework's present problems then Finally, a theoretical framework for developing an accurate IoT security solution offered. Khanna & Kaur [8] evaluates major contributions made by scientists across a range of application fields. In these articles, a number of criteria that were present in every application domain were examined. Also addressed are the present challenges in these areas. Tun et al. [9] provides a comprehensive analysis of the applications of wearable and Internet of Things (IoT) technologies, focusing on the types of data collected and the wide range of devices utilised in the field of ageing healthcare. This study presents novel opportunities for research in areas of emergent use, such as integrated applications and automated machinery, and also offers insights into areas of current IoT/wearable application. The analysis in this article may be useful to medical solution creators and creators in creating technology-backed prospective healthcare plans to fulfil the demands of the elderly and enhance their standard of life.

Babar et al. [11] offers a thorough examination of the subject of embedded security, especially in the field of IoT. In order to provide a flexible platform for adaptive early detection, proof of identity, assessments, isolation, and remedies versus successful breaches, the article highlights the requirement of integrating safety into the mobile device itself as a supplement to more traditional safety measures. After conducting the survey and analysis, the study determines the security requirements, taking into account the compute requirements, energy requirements, and memory requirements of the devices. The study concludes by recommending an embedded security structure as a part of the software/hardware co-design process.

3. Internet of Things (IoT) Framework

The Internet of Things architecture is divided into numerous layers, starting with the top application layer and ending with the edge technology layer at the bottom. These layers are constructed in such a way as to be able to satisfy the needs of numerous industries, businesses, governments, and other sectors. Below is a list of the functions that each tier of the architecture performs [8]. Figure 3 represents the layers of the IoT system.

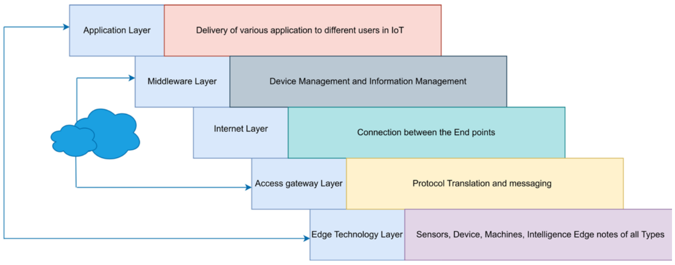
Application Layer
Delivery of various application to different users in IoT
Middleware Layer
Device Management and Information Management
Internet Layer
Connection between the End points
Access gateway Layer
Protocol Translation and messaging
Edge Technology Layer
Sensors, Device, Machines, Intelligence Edge notes of all Types

Figure 3: Architecture of an IoT System

(a) Edge Technology Layer: All of the hardware components, such as sensors, RFID tags, readers, or other soft sensors, as well as the device itself, are included in this layer. These are the main components of the data sensors that have been created in the field for monitoring or sensing various phenomena. By tying together devices on the network and the server, this layer is crucial to data collection.

(b) Access Gateway Layer: This layer aids in bridging the gap between two endpoints, such as a client and a device. This layer is where the very first data handling happens. It handles message routing, message identification, and subscribing.

(c) Internet Layer: The interaction between two end points, such as device-to-cloud, device-to-device, back-end data-sharing, and device-to-gateway, is carried out primarily by this layer, making it a significant layer.

(d) Middleware Layer: One of the most important layers that functions in two-way mode are this one. As its name implies, this layer functions as an interface between the hardware layer and the application layer because it resides between the two. It is in charge of crucial tasks including data management, device administration, and a number of other things like access control, data analysis, data aggregation, and data filtering.

(e) Application Layer: This layer, which is located at the top of the stack, is in charge of providing services to the appropriate users from various industries, including construction, manufacturing, automotive, security, and healthcare.

4. IoT Technologies and communication protocols

A variety of modern innovation and abilities are present on the lot. The IoT industry's difficult issue is the inexperience of both the vendors offering the services and the technologies with which they are related. They provide a significant obstacle for the businesses taking advantage of the land. IoT mostly makes use of networking standards and protocols for a successful communication between two endpoints [9].
Regarding the distance between a source and a destination, the main communication methods and protocols are as follows:

4.1 Wireless Short-Range Communication

(a) BLE (Bluetooth Low Energy): Bluetooth Smart, often called as Bluetooth LE, is a wireless LAN technology. Applications for this technology are planned across several industries including entertainment, security, healthcare, and fitness and entertainment.

(b) Light-Fidelity (Li-Fi): Only the speed and communication method distinguish Li-Fi through WiFi. Li-Fi is a system for Visible Light Communications (VLC) system that transmits data at an extremely fast rate of 224Gbps using regular in-home light bulbs [9].

(c) Near-field communication (NFC): NFC employs magnetic field induction to allow communication over a short distance between two electrical devices. It is mostly utilized in connectionless mobile payments, social networking, and document or product identification.

(d) QR codes and Barcodes: Both barcodes and machine-readable tags known as QR codes are used to carry information about the thing or thing's owner. In contrast to barcodes, which are available in both one-dimensional (91d0) and two-dimensional (2) formats, QR codes , or quick response codes, are two-dimensional codes that hold product information and may be scanned using smartphones.

(e) **RFID: Radio Frequency Identification:** RFID makes use of electrostatic field to read tags that contain data. RFID is employed in a variety of industries, including agriculture, veterinary medicine, livestock, and office environments.

(f) **Thread:** For loT devices, a networking protocol based on IPv6 is called thread. Its primary goal is residence automation, which will let the gadgets to talk to one another over local wireless networks.

(g) **Wi-Fi:** Wi-Fi is extensively used in wireless local area networking, also known as LAN. The 802.11n Wi-Fi standard, with a top speed of 600 Mbps and a maximum range of around 50 metres, is the most widely used one right now in homes and businesses.

(h) **Wi-Fi Direct:** Without a wireless access point, peer-to-peer communication using Wi-Fi Direct is feasible. The Wi-Fi direct devices don't actually start talking until they decide which device will act as an access point**.**

(i) **Z-Wave:** Mainly used for home automation, Z-Wave is a short-range, low-power communication system. It offers a quick and dependable way to remotely monitor and operate home appliances including HVAC, thermostats, garage doors, home theatre systems, and more.

(j) **Zig-Bee:** Another one is this short-range communication standard, which is based on IEEE 203.15.4. Zig-Bee should be used by devices that often send little amounts of data over short distances (10 to 100 meters) at low data rates [9].

4.2 Medium Range Wireless Communication

(a) **HaLow:** This Wi-Fi standard variation has an increased range, making it practical for connectivity in remote places. It provides modest data rates, which lowers transmission costs and power consumption [9].

(b) **LTE-Progressed:** LTE-progressed is a mobile communication standard that improves LTE by putting more emphasis on greater data rates, longer ranges, efficiency, and performance.

4.3 Long Range Wireless Communication

(a) Low Power Wide Area Networking (LPWAN): LPWAN refers to a class of wireless telecommunications systems that were developed to provide long-distance communication between two end stations. There are several LPWAN protocols and technologies available, including:

- **LoRaWAN**: Low Power Wide Area Network (LoRaWAN) is used for a variety of applications, such as mobile, industrial machine-to-machine, and secure two-way communications for Internet of Things (IoT) devices, smart cities, and healthcare applications [9].
- **Sigfox:** Used in gadgets with little data transfer needs and low battery lives.
- **Nuel:** In a tiny area of the TV white space spectrum, it is utilised to transmit high-quality, high-power, and affordable networks.

4.4 Wired Communication:

The type of network protocol that is currently most extensively used is Ethernet. It is a specific type of local area network (LAN), which denotes a networked connection of computers in a small structure, office, or on a campus. A type of network protocol called Multimedia over Coax Alliance (MoCA) sends high-definition video of a home and materials related to it over an already-existing coaxial cable.

- Electricity-line Communication (PLC): This protocol type transmits data and power via electrical cables. PLC is required for many applications, including those requiring industrial machinery, broadband over power lines (BPL), and home automation [9]

5. The role of operating system in loT Devices

Hardware and software are both included in loT devices. While operating systems are considered software, end devices and gateways are considered hardware. Due to an increase in hardware production (gateways, sensor nodes, etc.), traditional loT devices that previously operated without an OS started implementing new OS implementations that are tailored specifically for loT devices. These operating systems give the devices communication, usability, and compatibility [10].

Here are a few of the operating systems that a lot of devices use:
1. RIOT OS: It uses energy effectively and requires fewer resources. It can function on sensors, actuator boards, embedded systems, etc.

2. ARM mbed OS: This operating system is mostly utilized in low-power gadgets like wearables.

3. **RealSence OS X:** Intel's depth-sensi technology uses RealSense OS X. As a result, it is used in sensors, cameras, etc.

4. Nucleus RTOS: Mainly utilizing in industrial, medical, and aerospace applications.

5. Brillo: This embedded OS, which is based on Android, is utilized in inexpensive gadgets like thermostats.

6. Contiki: It is utilizing in low-power wireless gadgets like sound monitoring systems, street lighting, etc.

7. Zephyr: Zephyr is utilized in devices with limited resources and little power.

8. Ubuntu Core: Also known as Snappy, this software is utilized in edge gateways, robots, and other devices [10].

9. Integrity RTOS: Mainly utilized in the industrial, automotive, medical, aerospace, or defense sectors.

10. Apache Mynewt: It supports Bluetooth Low Energy-enabled devices.

6. IoT Device Management and attack Surface Considerations

Some of the IoT attack surface areas are as follows:

1). Device memory:

One of the most crucial parts of the IoT ecosystem is this. Memory is required by a gadget in order to store significant data about certain events. Some of the flaws in this component are covered in the sections below [11].

(a) Clear-text credentials

- **Vulnerability:** Credentials and information leakage from a device may be caused via unencrypted or clear-text credentials**.**
- **Consideration:** The communication between two end points should be carried out in an encrypted form to prevent it from being easily accessed to compromise it or gain unauthorized access to the platform. This will help keep the device and its information secure.

(b) Third-par credentials

- **Vulnerability:** One can access and take advantage of a device using third-party credentials.
- **Consideration:** Only a limited number of functions should be accessible to third parties, and their credentials should be encrypted using strong encryption software so that, even if a hacker were to obtain them, they could not be used to decrypt the credentials and gain access to the device.

(c) Encryption keys

- **Vulnerability:** Hackers can acquire encryption keys, which they can use to gain illegal access to the device**.**
- **Consideration:** The encryption key must be safeguarded against hackers using an appropriate key management system. The encryption key shouldn't be kept on the same computer as the data it decrypts; otherwise, if that computer is hacked, the keys are too.

2). Access control for ecosystems:

(a) Implicit confidence between parts

- **Vulnerability:** Because of unconscious belief, malevolent components may be trusted, which could cause all the components to malfunction**.**
- **Consideration:** Before engaging in interaction, each component should verify their own identity with other components. If relationships based on trust are formed, there should be robust mechanisms and procedures in place to ensure that the trust cannot be abused [11]**.**

(b) Enrolment security

- **Vulnerability:** Enrolling the device without certain limitations or an authentication mechanism may lead to the addition of a malicious device that could jeopardize the security of the network.
- **Consideration:** Each device should authenticate itself before getting enrolled.

3). Device web Interface:

(a). SQL injection

- **Vulnerability:** In order to extract and manipulate the database material, malicious code is injected into the application using the code injection technique known as SQL injection**.**

- **Consideration:** Using prepared statements and parametrized queries is a powerful SQL injection mitigation approach.

(b). XSS or Cross-site scripting

- **Vulnerability**: XSS, or cross-site scripting, is a type of attack that targets web applications and allows an attacker to insert malicious code to gain access to the system without authorization [11].
- **Consideration:** carefully observing and verifying inputs that are believed to be unreliable and ins data originating from an unreliable source.

(c) Cross-site Request Forgery

Vulnerability: This kind of attack uses a malicious website, blog, instant message, or application to make a user's web browser behave strangely on a reputable site for which the user is currently authenticated.

Considerations: Adding extra authentication information into requests to help the web application identify requests coming from unknown sources.

(d) Username enumeration

- **Vulnerability:** The use of the lost password form by an attacker to determine if a username already exists or not is known as user enumeration. They can utilize them to gain additional access to their accounts if they have a set of active or current usernames.

- **Considerations:** Applications should specify their own user names and should not be predictable. CAPTCHA can also be used, to an extent, to prevent user enumeration**.**

(e) Weak Passwords

- **Vulnerabilities:** An attacker can quickly access users' private and confidential information by brute forcing passwords that are weak or simple to guess.

- **Considerations**: Use strong passwords with lowercase, capital, alphabetic, and numeric characters. Dictionary words should also not be used as passwords because they are simple to guess.

(f) Account Lockout

- **Vulnerability:** Account lockout mechanisms are meant to guard against brute force password guessing attacks that could compromise the system's Account Lockout. Without a lockout mechanism, a user's account could be accessed by an attacker who could then access his or her personal information by brute forcing the password.

- **Consideration:** Considerations: A proper lockout mechanism should be put in place that locks out a user's account after three to five failed attempts to log in for a specific length of time.

(g) Known Default Credentials

- **Vulnerability:** Default credentials can be easily cracked and obtained if they are not changed, creating a vulnerability. Users should update the passwords on any gadget they purchase to avoid it falling into. the wrong hands and allowing unwanted access.

- **Consideration**: Users should change the passwords on any gadget they buy to guard against unwanted access.

7. Security Threats in IoT environment

Inadequate security protection principles are present in Internet of Things devices connected to the internet to counter numerous new threats. At an alarming rate, these gadgets are becoming infected with malware or harmful code. Attackers

frequently take advantage of these online devices with weak security to disrupt online traffic with DDoS attacks, intercept communications, and physically harm networks [10].
Some of IoT attacks are listed below:

1. DDoS Attack: To attack a particular system or server and prevent it from offering services, the attacker turns the devices into an army of Botnets.
2. Exploiting HVAC: Attackers take use of HAVC system flaws to get access to private data, including user passwords, and launch additional attacks on the target network.
3. Rolling code: The signal is jammed and sniffed by the assailant in order to obtain the code sent to the vehicle's receiver and use it to unlock and steal the vehicle.
4. BlueBorne Attack: In order to compromise the device, the attacker connects to adjacent devices and takes use of Bluetooth's flaws.
5. Jamming Attack: Attacker blocks communication between sender and receiver by flooding the channel with malicious traffic.
6. Remote Access using Backdoor: Attacker uses the IoT device as a backdoor to enter the organization's network by exploiting vulnerabilities in the device.
7. Remote Access using Telnet: An attacker takes advantage of an open telnet port to access shared information between connected devices, such as their software and hardware models [10].
8. Man-in –Middle attack: When communicating with a recipient, an attacker poses as a legitimate sender and intercepts all of their correspondence.
9. Ransomware Attack: A sort of malware known as ransomware uses encryption to prevent users from using their devices, either by locking the screen.

10.side channel Attack: Intruders carry out session hijacking by watching the emission of signals, or side channels, from IoT devices in order to gather information about encryption keys.

8. Software and Firmware Vulnerabilities in IoT System

Some of IoT vulnerabilities are mentioned below:

1. **Insecure Web Interface:** Weak credentials, account deficiency, lockout mechanisms, and account enumeration are just a few of the problems that might lead to an insecure online interface. Data loss, privacy invasion, a lack of responsibility, access denial, and total device takeover are the consequences of these problems.

2. **Insufficient Authentication/Authorization**: Insufficient authentication is the use of weak credentials, such as a weak password, which provides poor security and enables a hacker to access the user account, leading to data loss, account inaccessibility, and denial of access to the account for the user.

3. **Insecure Network Services:** Insecure network services are vulnerable to a number of assaults, such as buffer overflow attacks, which result in a denial-of-service scenario and render the user's device inoperable. To find open ports and exploit them for unauthorised access to the services, an attacker uses a variety of automated tools including port scanners and fuzzers.

4. **Integrity Verification and Transport Encryption are lacking:** Without using message encryption techniques, data can be easily intercepted and viewed during transmission, leading to information loss. Based on the revealed data, IoT devices or user accounts may also be compromised.

5. **Privacy Concerns**: IoT devices produce some private and confidential data, but because there is no adequate protection system in place, this creates privacy concerns and makes it simple to find and examine the data that is being generated, delivered, and gathered.

6. **Insecure Cloud Interface**: When simple-to-guess login credentials are used for a user account, an unsecure cloud interface is accessible. In order to gain access to data or take over the user account, a hacker takes advantage of the inadequate authentication system and absence of suitable transport encryption.

7. **Insecure Mobile Interface:** If account enumeration is possible and the login credentials are simple to guess, the mobile interface is insecure. Simply checking the wireless network connection will reveal any unsecured mobile interfaces.

8. **Insufficient Software/Firmware**: This type of problem developed when an IoT device's user was unable to alter the security settings, which increased the device's vulnerability and made it an easy target for hackers to exploit**.**

Table 1: IoT related vulnerabilities

9. Suggested Solution for Vulnerabilities in IoT System

IoT technology has advanced quickly without giving proper thought to the security of the devices. The risk of potential cyberattacks, the theft of confidential information, invasion of privacy, etc. is rising quickly as a result of the security flaws in

IoT devices. Before integrating the IoT system and products into an infrastructure, engineers or security experts must test the devices for a number of vulnerabilities. Some of IoT solutions are as given below.

Table 2: Suggested solutions for IoT security

10. Internet of things (IoT) Application Areas

There are numerous uses for the internet of things. They are employed in practically every field of society to help with a variety of chores that reduce normal job and private tasks and raise living standards. IoT technologies are used in smart buildings and houses, medical equipment, industrial appliances, security systems, and retail establishments, among other things [11].

IoT devices can be used for the following purposes:

- The thermostat, lighting system, security system, and a wide range of other systems installed in buildings are examples of smart devices that are connected to the internet and provide various services to end users.
- Devices including implanted pacemakers, ECG, EKG, surgical instruments, telemedicine, and other health monitoring technologies are used in the healthcare and life science sectors.
- The industrial internet of things (IIoT) is generating new growth through three strategies: boosting revenue-generating output, utilizing intelligent technology that is fundamentally altering the manufacturing process, and developing new hybrid business models.
- The notion of vehicle-vehicle, vehicle to roadside, and vehicle to pedestrian communication is used in the transportation industry when using IoT technology, which improves traffic situations, navigation systems, and parking plans [11].
- IoT is mostly utilized in retail for payments, advertisements, and tracking or monitoring products to prevent loss and theft and to boost sales.
- IoT devices in IT and networks mostly comprise of various office equipment including printers, fax machines, copiers, as well as monitoring PBXs, increasing communication between endpoints and facilitating the transmission of data over long distances [11].

Table 3: Application Areas of IoT.

11. Challenges and Drawbacks of existing IoT Security Approaches

The Internet of Things (IoT), which includes connected automobiles, smart homes, factory automation, and healthcare monitoring, has fundamentally altered the manner in which we communicate with our surroundings. IoT offers previously unheard-of comfort, productivity, and creativity, but it also comes with a variety of security vulnerabilities that, if not addressed, could have detrimental effects.

Due to their connectivity and widespread use, IoT devices have grown into appealing targets for criminals and other undesirable actors. To safeguard the IoT ecosystem, many security measures have been developed and implemented. The security and confidentiality of Internet of Things gadgets and information are jeopardized by a number of problems, and these present solutions are far from ideal [12].

In this comprehensive examination, we explore the intricacies of IoT security and draw attention to the shortcomings and constraints of the currently used security solutions. Because of the complexity of the issues, better knowledge and original solutions are required. It range from limited resource devices to dispersed networks and complicated regulatory systems [12].

Table 4: Drawback of Existing IoT security Approaches

12. Proposed Approaches in IoT security Enhancement

The security of linked devices and networks is more crucial now that the Internet of Things (IoT) has an important effect on every aspect of our lives. From automated, connected homes and industries to connected healthcare and transportation, the rapid growth of IoT has created both opportunities and difficulties that were previously unimaginable [12]. A key issue among these difficulties is maintaining the privacy and validity of IoT ecosystems. IoT is a networked technology, which presents vulnerabilities that could be abused by malicious parties, potentially leading to terrible outcomes such as data breaches, service failures, or even bodily harm. To deal with these security challenges, a comprehensive approach that incorporates both reactive and proactive strategies is required.

In this review study, we present a variety of proposed approaches to improve IoT system security. The main elements on which we focused are secure device activation and authentication. By enhancing the processes by which Internet of Things (IoT) gadgets join networks and verify their identities, we want to lessen the risks associated with unauthorized access, data breaches. These proposed methods cover a wide range of approaches and best practices, from touchless provisioning and collaborative authentication to device identity management and continuous monitoring [12]. By putting these methods into practice, we hope to give IoT stakeholders a comprehensive roadmap that emphasizes the different ways they may secure their IoT installations and protect the further development of related technologies. Let's now discuss these concepts for securing the Internet of Things device setup and identification in more detail. In Figure.4 we can see some proposed approaches for IoT security is shown.

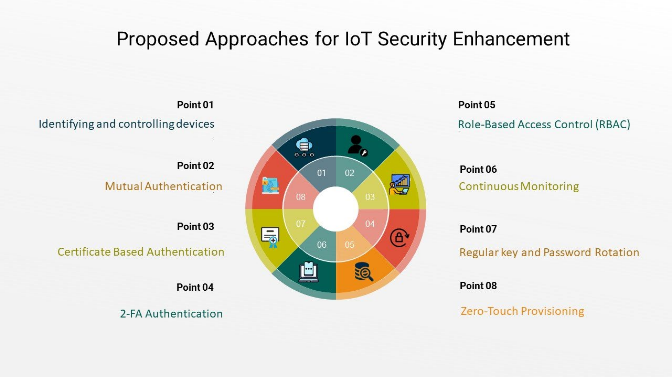
Proposed Approaches for IoT Security Enhancement
Point 01
Identifying and controlling devices
Point 02
Mutual Authentication
Point 03
Certificate Based Authentication
Point 04
2-FA Authentication
Point 05
Role-Based Access Control (RBAC)
Point 06
Continuous Monitoring
Point 07
Regular key and Password Rotation
Point 08
Zero-Touch Provisioning
01
02
03
04
05
06
07
08

Figure 4: Proposed Approaches in IoT Security Enhancement

1. **identifying and controlling devices**

- Upon provisioning or manufacturing, every IoT device will be given a unique identification and set of credentials in this way.
- To securely store device IDs and keys, use hardware with a high level of security, such as Trustworthy Platform Modules (TPMs).
- To prevent cryptographic keys from being readily altered or stolen, TPMs offer a safe environment for storing them.

2. **Mutual Authentication**

- Whenever there is a data exchange, the Internet of Things (IoT) device that the Internet connection or cloud service authenticate each other through mutual authentication.
- The device must validate the internet connection or service's trustworthiness to prevent unauthorized access, and vice versa.
- The parties typically exchange characteristics like certificates or licences during a handshake procedure to establish trust.

3. **Certificate Based Authentication:**

- IoT device security is typically provided through X.509 digital certificates.
- A trustworthy Certificate Authority (CA) should provide a unique certificate for each IoT device.
- The gadget displays its certificate as part of the authentication procedure to demonstrate its legitimacy.

4. **2-FA Authentication**

- By compelling the device to pair everything it owns with everything it knows (such as a tangible token or certificate), 2FA adds an extra degree of protection.
- To effectively authenticate, a device might, for example, be required to submit both an identification code and a certificate.
- Attackers will find it harder with this technique to acquire unauthorized access.

5. **Continuous Monitoring**

- Real-time observations of device behaviour and network traffic patterns are part of continuous monitoring.
- Automated detection of anomalies or questionable behaviour.
- To immediately address any security threats, automated alerts and actions are put up

6. **Role-Based Access Control (RBAC)**

- RBAC restricts device access privileges in accordance with roles and responsibilities.
- Each IoT device has a distinct role that outlines the access privileges for that device.
- By ensuring that devices have access to the resources needed for their intended functions, this reduces the attack surface.

7. **Regular key and password rotation:**

- It is necessary to enforce regular password and cryptographic key rotation procedures in order to lessen the impact of potential breaches.
- Human error is less frequent when key rotation is automated.
- Changing passwords and encryption keys on a regular basis can assist block attackers from using hacked data for a longer period of time.

8. **Zero-Touch Provisioning:**

- Zero-touch provisioning enables devices to automatically get their credentials and securely join to a network.
- Two examples of methods that can be used are Security Device Enrollment Protocol (SDEP) and Pre-Shared Key (PSK) provisioning.
- With SDEP, devices may safely get authentication information from a central authority, reducing the risk of being intercepted during provisioning.

13. Graph Neural Network (GNNs) in IoT Security

13.1 Introduction to GNNs

In recent years, graph neural networks (GNNs), that can model and analyze structured data given as graphs, have gained increased notoriety. GNNs offer a novel approach towards intrusion detection throughout the larger picture of IoT security by making use of the naturally graph-like architecture of IoT networks [13]. Networked devices in an IoT environment can display complex relationships and connections thanks to a subtype of deep artificial neural network techniques called GNNs. Unlike standard neural network models, which struggle with graph data, GNNs are exceptional at identifying useful traits and trends from graphs, making them especially appropriate for IoT security applications.

13.2 The Benefits of GNNs for Intrusion Detection

When utilized towards IoT intrusion detection, GNNs offer several advantages, including:

a. Topology Awareness: Due to the way that GNNs naturally record network topology, they are capable of discriminating between normal and aberrant activity based on the links between IoT devices [14]. They can now spot attacks that profit from network architecture thanks to this.

b. Semi-Supervised Learning: GNNs can handle limited labelled data circumstances, which are common in IoT environments. GNNs can learn a combination of labelled and unlabeled information in order to adapt to changing threats.

c. Local and Global Context: Neural networks use information from neighbouring nodes to give local context while accounting for patterns throughout the entire network. This increases their ability to detect minute anomalies.

d. Extracting features: GNNs produce pertinent traits using the graph data, doing away with the necessity for manual feature engineering. This is highly useful in dynamic IoT environments [14].

e. Scalability: Due to its capacity to scale to support very large IoT networks, GNNs are an excellent choice for real-world IoT deployments.

13.3 Mitigating IoT Security Challenges through the applications of GNNs

There are numerous challenges and concerns that threaten to seriously jeopardize the dependability and efficient operation of Internet of Things (IoT) networks in the constantly growing field of IoT security. Unauthorized access, breaches of information, and compromise of crucial infrastructure components are only a few of the issues that these concerns encompass. In an effort to address these pressing security issues, Graph Neural Networks (GNNs) have come to serve as a source of inspiration and innovation [15].

For enhancing the safety environment in IoT networks, deep learning-driven GNNs have demonstrated great promise. They have developed their program across a number of key axes, each focusing on a different facet of IoT security. As we can see in figure 5 steps for mitigating IoT security challenge is shown in figure 5.

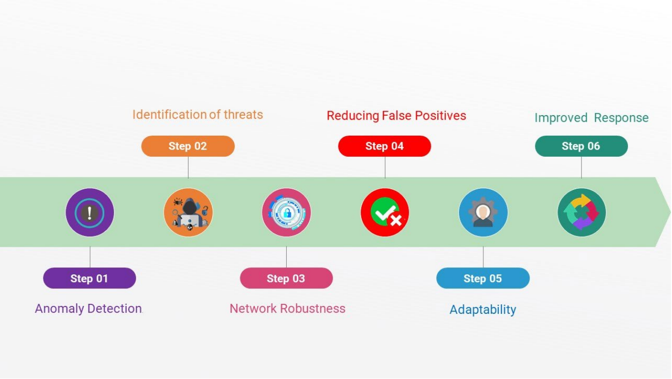

Figure 5: Steps for Mitigating IoT security challenges through the Applications of GNNs

Anomaly Detection: In IoT networks, GNNs are particularly effective at finding anomalies. They can accomplish this by directly ingesting the intricate graph-based representation of the Internet of Things (IoT) system and gaining a solid understanding of how various devices are connected. With such a thorough understanding, GNNs can recognize patterns that signify typical IoT ecosystem behavior [15]. As a result, when deviations from these established patterns occur, GNNs can quickly and accurately recognize and alert to these anomalies. This vital skill also involves the ability to recognize a variety of anomalies, including unauthorized access attempts, odd traffic patterns, and unexpected and possibly hazardous device behaviors. This preemptive anomaly detection provides rapid insights to security employees, enabling them to act swiftly and precisely.

Identification of Threats: The usage of GNNs can help identify threats across IoT networks. IoT environments are inherently exposed to a variety of threats, encompassing both established attack vectors and fresh, emergent threats. Because they have an in-depth knowledge of the network's graph design and device behavior, GNNs can effectively classify and identify these risks. It requires being able to recognize well-documented attack patterns derived from prior data as well as adapt to unanticipated and zero-day attacks in order to defend IoT networks against ever-changing security dangers.

Network Robustness: IoT networks typically exhibit dynamic characteristics as a result of the frequent entry and exit of devices. Conventional intrusion detection systems may become confused by such dynamism, while GNNs overcome the challenges by boosting Network Robustness.

GNNs can detect alterations in the network's structure that can be signs of malicious activity because they are familiar with the network's architecture. The network is strengthened and becomes more resistant to various types of intrusions because to this topology awareness.

Reducing False Positives: Additionally, GNNs significantly aid in lowering false positives, which are a daily challenge for security operations. False-positive alerts can overwhelm security workers with an excessive amount of pointless notifications, leading to alert fatigue and diminished system efficacy. GNNs, on the other hand, are naturally able to simulate complex relationships and interactions across IoT devices, which dramatically reduces the likelihood of false-positive alerts. They are able to create warnings that are more precise and particular because to their understanding of the complex relationships within the network, which frees up security employees to focus their attention and resources on genuine security incidents.

Adaptability: IoT settings are continually evolving because to the constant emergence of new devices, vulnerabilities, and attack vectors. The ability to continuously assimilate information from incoming data and adapt to changing network dynamics and emerging threats allows GNNs to stay up with these developments. This adaptability is a priceless tool in the ever-changing field of IoT security.

Improved Incident Response: A further advantage of GNN-based intrusion detection systems is improved incident response. Instead of only flagging security incidents, GNNs offer a fuller, more nuanced perspective of them. By utilizing the graph structure and behavioral patterns analysis, security teams are provided with actionable information regarding the type, scale, or potential effects of security incidents [16]. With this information at their disposal, security professionals can respond swiftly and effectively, minimizing any potential harm caused by security issues within IoT networks.

In basic terms, graph neural networks serve as a flexible and comprehensive solution to handle the plethora of issues and difficulties relating to IoT security. The detection of anomalies, threat identification, network stability, false-positive reduction, flexibility, and incident response improvement are among their capabilities. As a result, GNN-based detection systems for intrusions are an essential tool for securing IoT networks by strengthening their defenses against a wide range of security risks and weaknesses.

13.4 Enhancing IoT Intrusion Detection with Graph Neural Networks (GNNs): From Data collection to Deployment

The application of Graph Neural Networks (GNNs) for IoT detection of intrusions offers a cutting-edge and adaptable technique to improve the integrity of IoT ecosystems. Let's get into the details of building up a system for intrusion detection (IDS) that employs GNNs and is specifically created for the unique challenges of IoT contexts. In the below figure 6 illustrates the IoT Intrusion Detection with Graph Neural Networks (GNNs) [18].

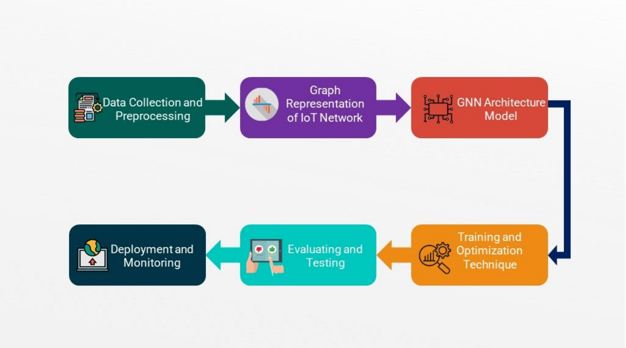
Data Collection and Preprocessing
Graph Representation of IoT Network
GNN Architecture Model
Training and Optimization Technique
Evaluating and Testing
Deployment and Monitoring

Figure 6: IoT Intrusion Detection with Graph Neural Networks (GNNs)

Data collection and Pre-processing

Data collection and preprocessing is the first stage in creating a successful IDS for IoT. Device logs, network activity, sensor readings, including historical security event records are just a few of the types of data that IoT networks produce. It's essential to recognize the different sources of data to make sure you get pertinent data from different gadgets and network elements. Data integrity maintenance requires data quality assurance [18]. This entails dealing with problems like values that are missing, outliers, and interference that could jeopardise your IDS's accuracy. Data entries with timestamps provide important temporal information, allowing you to analyze event sequences. Data labeling, which involves categorizing information events as normal or abnormal based on past data or professional knowledge, is crucial.

Graph Representation of IoT Network

Since IoT settings are inherently interconnected, describing the network as a graph is highly helpful for intrusion detection. In this step, the IoT network's hardware is given a graph node identity, and the interactions and connections between those nodes are represented as edges. By building an IoT network graph, the topology of the network is correctly depicted, showing how gadgets connect to and communicate with one another [19]. Device-specific details like the kind of device, IP address, and version of the operating system should be included in the features that are assigned to each node in a graph. Edge components that show how frequently or to what extent interactions between devices occur may also be present.

GNN Architecture Model
A GNN architecture must be carefully chosen if an IDS is to be built successfully. Depending on the characteristics and security requirements of your IoT network, you can choose between Graph Convolutional Networks (GCNs), GraphSAGE, Graph Awareness Networks (GAT), and Gated neural networks based on graphs (GGNNs). GNN layers are used to learn node embeddings, which represent device properties and their context across the IoT network [19].

The technique for distributing and aggregating data across the graph must be carefully chosen. It is necessary to specify a message-passing system, that may comprise attention techniques, recurrence updates, or graph convolutions. Create an output layer that, after learning the node embeddings and the graph structure, generates labels or scoring for intrusion detection.

Training and Optimization Techniques
A GNN design needs to be thoroughly thought out if an IDS is to be properly established. Depending on the characteristics and security requirements of your IoT network, you can choose from Graph Convolutional Networks (GCNs), GraphSAGE, Graph Awareness Networks (GAT), and gated neural network networks based on graphs (GGNNs). GNN layers are used to learn node embeddings, which represent device features and their context across the IoT network. A chart's data distribution and aggregation strategy must be properly chosen [20]. It is necessary to specify a message-passing system; it might contain attentiveness mechanisms, graph convolutions, or recurrence updates. After understanding node incorporation and the graph structure, create an output layer that generates labels or scores for intrusion detection.

Evaluating and Testing
Ensure the GNN-based IDS is adequately assessed to ensure its success. Use relevant performance metrics, such as precision, recall, and precision, as well as F1-score, ROC-AUC, or confusion matrices, to assess the model's performance. In order to make sure the IoT data is reliable and capable of identifying intrusions, test its accuracy and effectiveness using actual data. Compare the GNN-based technique to traditional IDS systems in order to highlight the advantages and improvements it offers.

Deployment and Monitoring
As soon as the GNN-based IDS has undergone validation, your IoT network can begin using it. Ensure the safety of your IoT ecosystem by putting in place reliable monitoring and alerting systems that can react quickly to identified incursions. To stay current with threats and preserve the efficient operation of your IDS in the changing IoT security environment, regular updates and model retraining are essential [20].

14. Conclusion

This paper gives a general description of the IoT system, such as its traits, architecture, different kind of IoT attacks, various security concerns, IoT related vulnerabilities, threats, challenges and potential application areas for IoT security. Additionally, this paper also provides a number of IoT solutions, challenges and drawbacks of existing IoT system, Proposed Approaches in IoT surety Enhancement. This paper also Discuses about Graph Neural Network GNNs in IoT security and Enhancing IoT Intrusion detection with Graph Neural Networks (GNNs). This field is still very young and developing. The technologies that make up the foundational infrastructure layers are progressing. The future applications of IoT is very wide, this technology is helping so much in healthcare, architecture and automotive industry. In the areas of communication technology and IoT applications, additional work must be done. These industries will surely mature during the next ten years and have an unfathomable impact on human life.

References

[1] Journal article: Mohamad Noor, M. B., & Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer Networks*, *148*, 283-294. https://doi.org/10.1016/j.comnet.2018.11.025

[2] Review paper: Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. *Computer Science Review*, *44*, 100467. https://doi.org/10.1016/j.cosrev.2022.100467

[3] Conference: Z. -K. Zhang, M. C. Y. Cho, C. -W. Wang, C. -W. Hsu, C. -K. Chen and S. Shieh, "IoT Security: Ongoing Challenges and Research Opportunities," *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, Matsue, Japan, 2014, pp. 230-234, doi: 10.1109/SOCA.2014.58.

[4] Article: Jurcut, A. D., Ranaweera, P., & Xu, L. Introduction to IoT Security. 27-64. https://doi.org/10.1002/9781119527978.ch2

[5] Conference Paper: R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, London, UK, 2015, pp. 336-341, doi: 10.1109/ICITST.2015.7412116.

[6] Conference Paper: Q. Gou, L. Yan, Y. Liu and Y. Li, "Construction and Strategies in IoT Security System," 2013

IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, Beijing, China, 2013, pp. 1129-1132, doi: 10.1109/GreenCom-iThings-CPSCom.2013.195.

[7] Article: N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702-2733, thirdquarter 2019, doi: 10.1109/COMST.2019.2910750.

[8] Review Paper:] Khanna, A., Kaur, S. Internet of Things (IoT), Applications and Challenges: A Comprehensive Review. *Wireless Pers Commun* **114**, 1687–1762 (2020). https://doi.org/10.1007/s11277-020-07446-4

[9] Review Paper: Tun, S.Y.Y., Madanian, S. & Mirza, F. Internet of things (IoT) applications for elderly care: a reflective review. Aging Clin Exp Res 33, 855–867 (2021). https://doi.org/10.1007/s40520-020-01545-9

[10] Conference: N. Shahid and S. Aneja, "Internet of Things: Vision, application areas and research challenges," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2017, pp. 583-587, doi: 10.1109/I-SMAC.2017.8058246.

[11] Conference: S. Babar, A. Stango, N. Prasad, J. Sen and R. Prasad, "Proposed embedded security framework for Internet of Things (IoT)," 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), Chennai, India, 2011, pp. 1-5, doi: 10.1109/WIRELESSVITAE.2011.5940923.

[12] Journal article: Cirne, André, Patrícia R. Sousa, João S. Resende, and Luis Antunes. "IoT security certifications: Challenges and potential approaches." *Computers & Security* 116 (2022): 102669.

[13] Journal article: Paricherla, M., Babu, S., Phasinam, K., Pallathadka, H., Zamani, A. S., Narayan, V., ... & Mohammed, H. S. (2022). Towards Development of Machine Learning Framework for Enhancing Security in Internet of Things. *Security and Communication Networks*, *2022*.

[14] Review article: Dong, G., Tang, M., Wang, Z., Gao, J., Guo, S., Cai, L., ... & Boukhechba, M. (2023). Graph neural networks in IoT: a survey. *ACM Transactions on Sensor Networks*, *19*(2), 1-50.

[15] Review article: Altaf, T., Wang, X., Ni, W., Yu, G., Liu, R. P., & Braun, R. (2023). A new concatenated Multigraph Neural Network for IoT intrusion detection. *Internet of Things*, *22*, 100818.

[16] Conference Paper: Baldoni, S., Battisti, F., Carli, M., & Neri, A. (2023, April). A context-based framework for enhancing GNSS performance and security. In *2023 IEEE/ION Position, Location and Navigation Symposium (PLANS)* (pp. 729-739). IEEE.

[17] Conference Paper: Baldoni, S., Battisti, F., Carli, M., & Neri, A. (2023, April). A context-based framework for enhancing GNSS performance and security. In *2023 IEEE/ION Position, Location and Navigation Symposium (PLANS)* (pp. 729-739). IEEE.

[18] Journal Article: Y. Zhang, C. Yang, K. Huang and Y. Li, "Intrusion Detection of Industrial Internet-of-Things Based on Reconstructed Graph Neural Networks," in *IEEE Transactions on Network Science and Engineering*, 2022, doi: 10.1109/TNSE.2022.3184975

[19] Journal Article: Zhang, Y., Yang, C., Huang, K., & Li, Y. (2022). Intrusion detection of industrial internet-of-things based on reconstructed graph neural networks. *IEEE Transactions on Network Science and Engineering*.

[20] Journal Article: Nguyen, H., & Kashef, R. (2023). TS-IDS: Traffic-aware self-supervised learning for IoT Network Intrusion Detection. *Knowledge-Based Systems*, 110966.