IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Security of The Embedded and IoT Systems: Threats, Attacks, and Countermeasures

Mohamed Kasim J.

B.E. (ECE) Undergraduate Student,
Department of Electronics and Communication Engineering,
Annamalai University, Chidambaram, Tamil Nadu, India.

Abstract: The **Embedded systems** help humans to live a convenient life. Most of the devices employed are altered to work smart for the requirements of humans. Embedded systems are most popularly used in the field of electronics, aviation, communication, health care, home appliances, and many more. With the increasing use of the embedded system devices in our day-to-day lives, security threats have also risen at a corresponding rate. However, assuring security in the embedded systems has become an extreme challenge for the embedded device professionals and the manufacturers of products. Security is always becoming a huge concern to the embedded system due to its drawbacks like power constraint, processing power, and cost. The latest trend of integrating the embedded systems with the internet introduces various vulnerabilities and exposes the attack surface of the embedded system. Incorporating networking capabilities may raise multiple attacks such as packet injection, Man In The Middle (MITM) attacks, and replay attacks. Hence, the security of these systems is very crucial to the sellers and consumers. The **Internet of Things (IoT)** technology helps humans to live a life with quality and comfort. IoT has contributed significantly to various application areas. The extensive development of smart electronic devices and their data transmission protocol using wireless mechanics boost their vulnerability to various cybercrime and attacks. Consequently, the rate of cybercrime is rising every day. Hence, the study of embedded and IoT system security threats and respective counteractive measures can benefit security researchers in identifying proper solutions to face the enormous challenges in cybercrime investigation. IoT forensics plays a vital role in the investigation of cybercrimes. Numerous security issues at each layer in the embedded systems and internet of things (IoT) are also discussed briefly. In this paper, the vulnerabilities and threats present in the embedded systems and internet of things (IoT) are discussed, along with the countermeasures for mitigating those attacks.

***Index Terms* - Embedded systems, Internet of Things (IoT), Cybercrime, Cyberattack, Security Threats, Countermeasures.**

I. INTRODUCTION

An Embedded System (ES) is an electronic-mechanical system designed to accomplish a certain function, and it is a mixture of both hardware and firmware(software). Every embedded system is distinctive, and the hardware and the software are highly specialized to the application domain. Embedded systems are becoming a crucial part of any device or equipment in all fields, including household electric appliances, medical equipment, industrial control systems, etc. An Embedded system (ES) is either a microprocessor or microcontroller-based system designed to perform certain work. The basic modern, real-time embedded computing system was the Apollo Guidance Computer, invented in the 1960s by Dr. Charles Stark Draper at the MIT Instrumentation Laboratory for the Apollo Program [1]. Embedded Systems are designed to operate with zero or minimal human interference, and they also become an indispensable part of human lives [2]. In the simplest form, the concept of an embedded system is demonstrated when a processing unit is integrated into a larger physical system to steer its functions. For many decades, embedded systems have gone through various stages of development until they have reached what they are today. The capabilities of embedded systems evolved in conjunction with various critical vital technologies. The most essential and common technologies are integrated circuits (ICs), such as Field Programmable Gate Arrays (FPGAs) and Application Specific Integrated Circuits (ASICs). The only difference between ASICs and FPGAs lies in the fact that FPGAs are reconfigurable, whereas ASICs must be pre-configured for the motive for which they are manufactured. The inclusion of Programmable Logic Controllers (PLCs), microcontrollers, and microprocessors during the developmental cycle of embedded systems played a significant role in advancing the capabilities of embedded systems allowing them to be employed in a large variety of applications. Embedded systems have shown massive potential in IoT network-connected systems with the evolution of IoT [3]. Based on the requirements of the user, manufacturers can develop embedded systems that are easily configured and programmed. The embedded systems play a vital role in the Internet of Things (IoT) systems due to distinctive features and functions like less power consumption, reactive computing, low general and operating expenses in embedded systems. The significant difference between embedded systems and IoT is that most embedded systems software are never changed once programmed, and they are typically small software programs. On the other hand, the IoT software program gets updated at regular intervals. They are generally complex software programs that involve cloud computing, big data analytics, and others. Because of regular updates, IoT systems maintain their quality and performance.

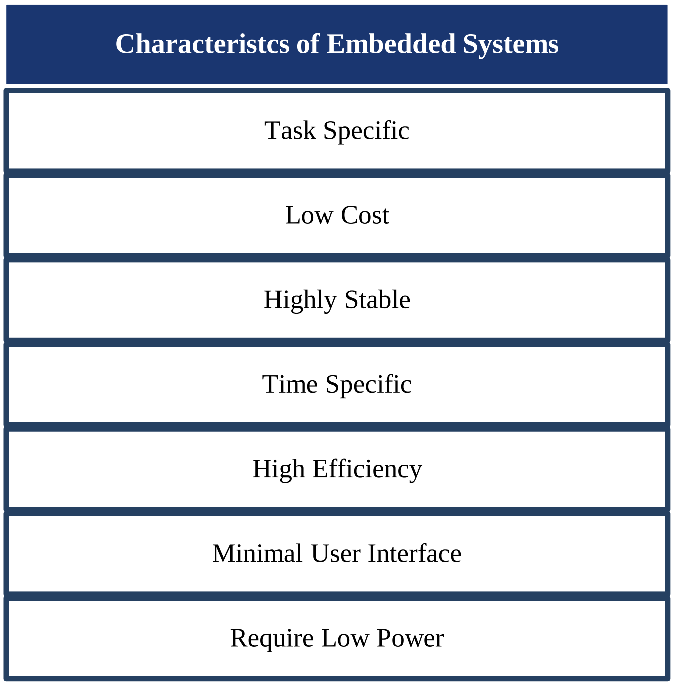

Figure 1: Characteristics of Embedded Systems [2].

The **Internet of Things (IoT)** platform connects heterogeneous devices or systems over the network. The rapid development in technologies has resulted in automation and real-time analytics being applied across various interesting fields such as wildlife monitoring, agriculture, military, healthcare, manufacturing, transportation, supply chain, and inventory management. Internet connectivity has become a basic essential around the earth where IoT connects more than billions of people by mobile devices, giving rise to immense processing power, storage capabilities, and knowledge access throughout the world. The interconnection of physical devices such as appliances, vehicles, and human beings with the help of sensors, actuators, and software leads to the formation of a network. This technique enables the physical devices to communicate, interact, process, and exchange data among themselves. The term "Internet of Things," which is also known as IoT, was coined back in 1999 by Kevin Ashton, the British technology pioneer who co-founded the Auto-ID Center at MIT [4].

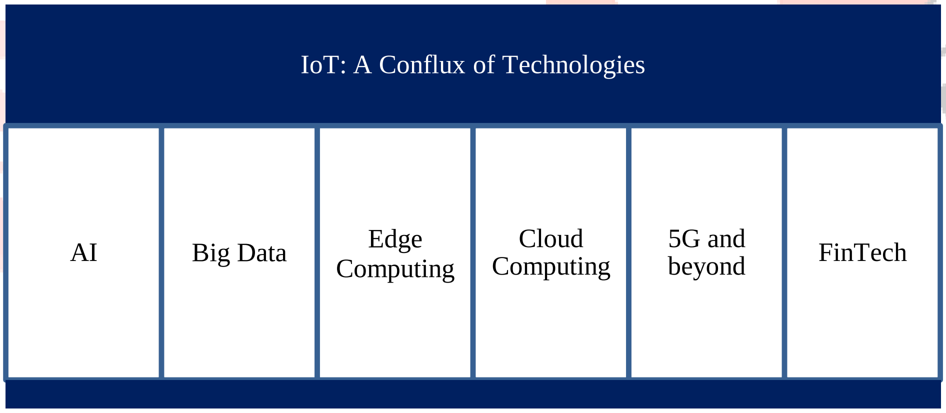

Figure 2: IoT: a conflux of technologies [5-9].

In a very short period of time, IoT has been expanded in many domains. Their applications range from simple household devices to very complicated and advanced industrial automation equipment and machines. Smart agriculture, supply chains, self-driving vehicles, smart homes, underwater IoT sensors, and smart industries with automation technology are some of the areas that have benefitted the most from the Internet of Things technology [5],[10],[11]. The Internet of Things has also converted a wide range of objects into devices that provide more lifestyle-friendly digitized services [12]. The attack surface for cybercrime is massively expanded due to the increase in the number of IoT smart devices connected through cyberspace [13].

II. Security Threats of Embedded & IoT Systems

A threat is an action that benefits security vulnerabilities in a system and negatively impacts it [14]. Threats can originate from two fundamental sources: nature and human beings [15],[16]. Natural hazards like earthquakes, tsunami, tornados, floods, and fire could cause heavy damage to computer systems. People can prepare some safeguards against various natural disasters, and nothing can prevent them from happening. Disaster recovery methods like backup and contingency plans are best to secure systems against various natural threats. Human threats are those created by people, such as many malicious threats consisting of internal threats (someone has legal access to the system) [17] or external threats (individuals or organizations functioning outside the system network) [18] seeking to harm and malfunction a system. As per Behrtech's cybersecurity stats, the cyberattacks on IoT have tremendously increased by 600% between 2016 - 2017. The total damage caused by cybercrime on the Internet of Things (IoT) will reach $6 trillion by 2021 annually. The IoT security spending to prevent cyberattacks worldwide will reach $3.1 billion [104].

Human threats can be classified into two types, and they are given below.

i. **Unstructured threats** consist of primarily immature attackers who perform the attack using the readily available hacking software tools on the internet.
ii. **Structured threats** as people know system weakness and can understand, develop and exploit programming codes and scripts. Advanced Persistent Threats, which is also known as APT, is a well-known example of structured threats [19]. APT is an advanced network attack targeted at high valuable data or information in business and government organizations, such as financial institutions, manufacturing industries, and national defence, to steal very important data or information [20].

Most embedded systems are highly susceptible to a massive range of security breach attacks. For example, a resource exhaustion attack could drain the power resource by rising computational tasks or the use of peripherals or sensors. Cyber attackers could also easily gain physical access to the embedded systems, so these systems are highly susceptible to massive physical attacks: if attackers have a physical approach to the system, they might conduct a physical intrusion, damage the integrity of the system, and/or execute snoop attacks on the system bus, as well as probably causing sensor or peripheral damage. The saved data or cryptographic keys of an embedded system or electronic currency on smart cards are susceptible to illegal access, and they must be secured to ensure the security of embedded systems. Besides, the embedded system's authenticity is constantly highly susceptible to several cyberattacks, like malicious data or information produced by the system's sensors, an unauthorized user, or illegal reprogramming [3]. Moreover, the Central Processing Units themselves do not have sufficient hardware protection against logical and physical attacks. A more Powerful CPU could mitigate many attacks, but these are overpriced and customarily limited to use on smart cards or as dedicated secure elements in System On a Chips. Assuming that the performance of the processor has been upgraded in accordance with the requirements of advanced encryption, this creates a new issue: the requirement for a significant amount of energy; for example, in the case of portable systems, it is hardly possible. However, if these two issues are resolved, we will face a new issue: the total cost. Even if only a few cents, a slight increase in the cost of production would be overpriced and would affect competitiveness if more than thousands of units were manufactured [3],[21].

Cybersecurity professionals usually try to find the attacker's capabilities to avoid cyberattacks. The capabilities of an attacker always depend on accessible and unprotected entry points on the attack surface of an embedded system. Hardware components like Wireless Fidelity (Wi-Fi), Bluetooth, Universal Serial Bus (USB) or other input/output interfaces, and software systems like operating systems (OS) or applications, increase the abilities and flexibility of embedded systems but may provide a larger attack surface for attackers or hackers; thus, the system becomes more susceptible for cyberattacks. In other words, if the capabilities of embedded systems increase in terms of the number of connections and input units, then attack surfaces increment, thereby expanding the probability that the system is hacked. The problem worsened due to the easy availability of advanced and low-cost physical attack tools like Chip Whisperer and Chip Shouter to perform side-channel attacks (SCAs) or glitch attacks [22].

Despite implementing highly secured password protection and encryption protocols like SSL (Secure Socket Layer) or SSH (Secure Shell) in every embedded system, it is not enough to make the system more secure and invulnerable to security threats. Numerous well-structured attacks have been successfully implemented on various embedded devices by the cyber attackers varying from toasters to vehicle control systems due to the vulnerabilities present in the system in the past. Enormous layers of protection like encryption, authentication, firewalls, security protocols, intrusion detection, and intrusion prevention systems usually protect enterprise data. Despite this, many embedded systems do not have any highly secured firewalls for protection and are only protected by passwords in maximum cases [23]. The unauthorized access to important confidential data, privacy breaches, misuse of secret information, and personal identity theft are some ethical problems in society caused by the evolution of IoT. Though these problems were existing in the internet's era and Information and Communication Technology (ICT), recently they have become more dominant on the Internet of thing (IoT) systems [38]. Most of the Internet of Things (IoT) devices are not designed with security in the first place, and many do not have traditional operating systems (OS) or even sufficient memory or processing power to integrate security features. Not only that, but IoT devices are developing in number, with over a million new devices connecting to the internet every day. The consequence is a massive quantity of data transferring freely between various devices and across network environments, remote offices, mobile workers, and public clouds with minimal visibility, making it hard to track and secure this data [47].

Attackers have many possibilities to enter the network of an organization due to the large attack surface of IoT systems and lack of inbuilt security features [47]. Most of the IoT industry does not have proper security standards or protocols for developers and manufacturers to build inconsistent security, but there are more security best practices. IT administrators might find it hard to keep track of and update devices, which can remain in the field for numerous years [48].

Initially, attackers examine the networks for devices and known vulnerabilities and increasingly use nonstandard ports to get access to the network. Once they have access to the device, it is simpler to avoid detection through fileless malware or software memory on the device. Figure 3 describes various potential risks associated with IoT systems.

Some of the cyberattacks that caused severe trouble to companies and industries are briefly explained below. Slammer, also known as SQLExp, caused massive damage to a nuke plant in the northeast of Oak Harbor of the United States. The simple piece of programming code present in that worm (a form of malware/virus) created more misfortune than anticipated. Initially, It deactivated the monitoring systems that were used for safety monitoring. Although the security system was in place, the attack happened. Cyber attacker initiated the attack from a contractor’s network that was linked with the plant facility. Fortunately, it did not pose any heavy damages [24]. Mirai botnet attack initially occurred on September 19, 2016. The meaning of the word "Mirai" in the Japanese language is "future." The attack aimed the networked embedded systems like IP-enabled cameras and routers with less secure passwords. The botnet created by these devices helped to launch a massive Distributed Denial of Service (DDoS) attack on a website that a computer security journalist owns. It was one of the worst attacks that trembled the whole internet [24].

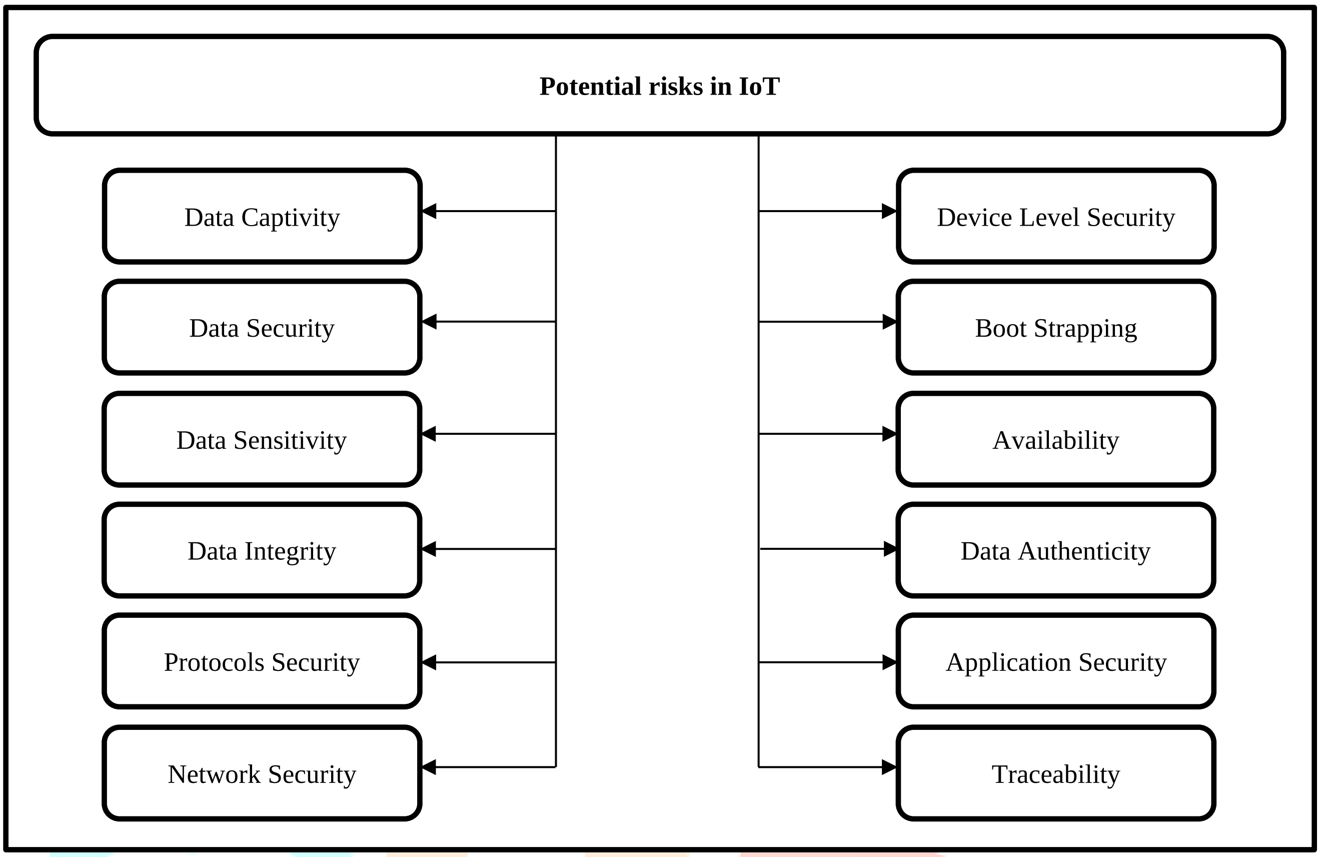

Figure 3: Potential risks in IoT [5],[38-43].

From the above incidents, one can understand the significance of security in embedded system design and implementation. Since IoT is the combination of technologies like embedded systems, real-time computing, actuation, and wireless sensor networks (WSNs), the security issues in the embedded systems cause various vulnerabilities in the IoT systems, which helps the attackers easily access the IoT systems. Hence, it is extremely important to research more on the security of embedded systems and create a framework to reduce the attacks.

III. Attacks on Embedded & IoT Systems

According to the cyber security report released by IBM, Human errors and carelessness are the significant vulnerabilities that cause various cyberattacks to take place, and human errors cause nearly 95% of cyber security breaches. About 19 out of 20 cyber breaches would be avoided if human errors were excluded [105]. Based on the Behrtech cybersecurity stats, in the industrial internet of things (IIoT), 54% of the organizations have experienced a minimum of one cyber-attack on their industrial control system over a year.

Attacks on embedded systems can be classified into three categories depending on their targets.

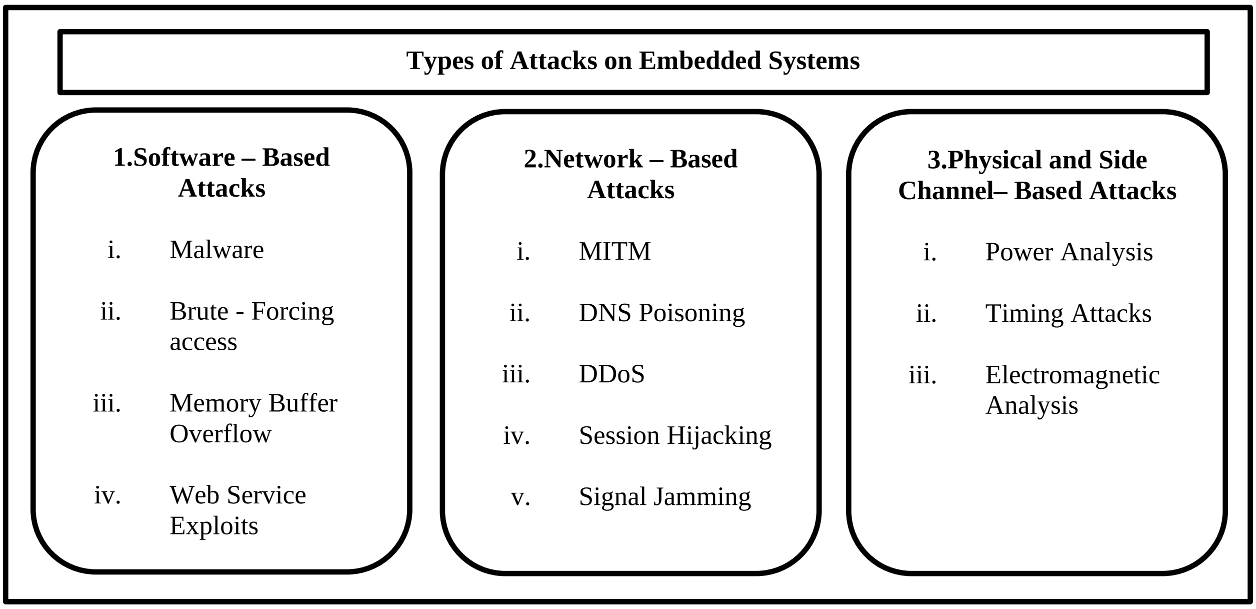
Types of Attacks on Embedded Systems
1.Software – Based Attacks
i. Malware
ii. Brute - Forcing access
iii. Memory Buffer Overflow
iv. Web Service Exploits
2.Network – Based Attacks
i. MITM
ii. DNS Poisoning
iii. DDoS
iv. Session Hijacking
v. Signal Jamming
3.Physical and Side Channel– Based Attacks
i. Power Analysis
ii. Timing Attacks
iii. Electromagnetic Analysis

Figure 4: Types of attacks on embedded systems [24], [25].

1. Software-based attacks:

Software is one of the primary parts of an embedded system as it acts as a brain for the system. Most of the security threats arise in software applications. Without including the secure coding concepts, improper coding in the design phase may inherit security threats such as buffer overflow, memory stack attacks, and injection attacks [24]. If an attacker can access important sensitive data or gain control over an embedded system, it is considered a successful attack on its software. Searching for security threats in software design and code is the most popular attack vector because it's possible to conduct software-based attacks remotely [25]. Some of the most important software-based attacks are given below.

1.1 Malware:

Malware attacks on embedded systems always work similarly to any other system: a hacker deploys a piece of malicious programming code that tries to hijack the data saved inside the system, take authority over the victim system, or harm it. Most Hackers fake firmware updates, drivers, or security patches to distribute malware which is malicious code [25]. The IoT and embedded systems are the significant targets of malware. Most malware gets into the system by downloading the erroneous files and executing the executable and firmware update. The user must be aware of the source from which they download the firmware updates and patches for embedded systems [24],[26].

1.2 Brute Force:

Brute force is the technique by which the attacker tries all the combinations of passwords or passphrases from a known dictionary file or word list. Most of the embedded systems give remote access to the users through a Graphical User Interface (GUI). The access control mechanism for the interface is only through authentication of the password. Hence, if the system user sets the default password or weak password, it becomes much easier for the attacker to gain authority over the system. This technique allows weak crypto algorithms and authentication mechanisms to be easily cracked [24],[27].

1.3 Memory Buffer Overflow:

If the attackers manually overflow the memory buffer in an embedded system assigned to contain data, this form of cyberattack is well-known as a Memory buffer overflow attack. Hackers use vulnerabilities present in the memory buffer of an embedded system to fill an enormous amount of data. In this case, an embedded device's operating system (OS) will allocate excessive data to memory sections adjacent to the buffer. This excessive data may contain shellcode, malicious code, or other exploits that help cyber attackers obtain credentials of the system and elevate their access rights [25].

1.4 Web Service Exploits:

Many embedded systems have a web server build into them to serve the user with GUI controls. Hence, it indirectly acquires all the vulnerabilities from the webserver. Therefore, hardening the webserver by closing the unnecessary ports of the system is very important. Code injection like Structured Query Language (SQL) injection will make the system more vulnerable to illegal authentication and leakage of important sensitive data [24],[28].

2. Network-based attacks:

Capabilities of the network help the user to manage the system and control it remotely. They also acquire the networking infrastructure vulnerabilities like Man In The Middle (MITM) attacks, packet injection, and replay attacks [24]. Cyber attackers can easily listen for, intercept, and modify network traffic that is transmitted by an embedded system using these security vulnerabilities [25]. Some of the most significant network-based attacks such as MITM, DNS Poisoning, DDoS, Session hijacking, Signal jamming are explained below.

2.1 Man in the Middle (MITM) Attack:

MITM is a well-known network-based attack in which the hacker redirects the traffic through their computer system using techniques like Address Resolution Protocol (ARP) poisoning. The weak encryption will make it much easy for the hacker to interpret the data. All the data from the system will pass through the hacker system. Hence, it creates an opportunity for the hacker to customize the data and compromise the system's integrity [24],[29].

2.2 DNS Poisoning:

The hacker may poison the local Domain Name System (DNS) server to customize the records to their needs. When the system tries to send data to a legitimate website, the hacker will redirect it to their website due to DNS poisoning. Hackers can host a fake webpage/website to gather user credentials such as username, password, and data. Using protocols like Domain Name System Security Extensions (DNSSEC) will help in mitigating the risks [24],[30].

2.3 Distributed Denial-of-Service (DDoS) Attack:

The DDoS attack consists of numerous computer systems controlled by the attackers to attack and cause a denial of service to the user of the targeted system. The attacker's target can be a system, server, website, or another network resource. As a result, the enormous amount of incoming messages, connection requests, or malicious packets overflows the target system and forces the system to run slow, crash, or even shut down, which turns down the services to legitimate users or systems. The attackers mostly carry out the distributed denial-of-service (DDoS) attacks, ranging from individual criminal hackers to organized crime rings and government agencies [31].

2.4 Session Hijacking:

The various authentication methodologies are mostly integrated with sessions to control the access and bring state during communication. The hacker will use attacks like MITM (Man In The Middle) before going for session hijacking. When the data pass through the attacker network, the hacker can use software tools to capture the session, and it is reused for the authentication process [24],[32].

2.5 Signal Jamming:

Signal jamming is when the hacker jams the signal by making interference and distortion of the actual signal. It happens mainly in the wireless mode of communication. This attack compromises the availability of the embedded system as the system will be incapable of sending and receiving the data [24],[33].

3. Physical and Side-channel based attacks:

Cyber attackers can easily launch physical attacks by using various probe tools available in the market and eavesdropping on the data transmitting between the interconnections. Most of the embedded systems use advanced techniques to safeguard from physical attacks such as obfuscation. The hacker needs to unpack, reconstruct and analyse the components of the system. Hence, it requires a massive amount of expertise in the hardware system. These hackers are highly expensive and hard to perform. The side-channel-based attacks are launched with the help of the information revealed by the systems, such as timing, power consumption, and electromagnetic leakage. It gives information on the internal operation of the system that can aid the attacker in solving his riddle-like finding the cryptographic keys [24]. Some of the most important physical and side-channel-based are enumerated below.

3.1 Power Analysis Attack:

The power consumption of a device is represented by the switching activities inside the hardware circuit. It may help the hacker infer the cryptographic algorithms and crypto keys since the switching depends on the data available in the system. This type of cyberattack needs physical access to the device and probing of the connections. These attacks are known as power analysis attacks. They can compromise the embedded systems like a smart card system [24],[34].

3.2 Timing Attacks:

The timing attacks exploit the timing of execution of the cryptographic algorithm to detect the keys and algorithms used underneath. This is because the computational timing is always directly proportional to the cryptographic key. The variation in the hardware architecture may present different values for different systems. Hence, it requires in-depth knowledge of different architecture to use this technique [24],[35].

3.3 Electromagnetic Analysis Attacks:

By calculating the electromagnetic radiation from the chip, it can identify the sensitive data from the system. Knowledge of the system layout is needed to exploit the system using this kind of attack. As there will be much interference around the system, isolation must be performed in order to obtain the data. The charge of implementing this attack is comparatively much higher, and the equipment is highly priced [24],[36].

Common attacks on IoT Systems – The IoT systems are susceptible to various attacks due to their inherent vulnerabilities. The common cyber-attacks on IoT systems are explained below.

1. **Physical attacks :** This kind of attack tampers with hardware components of IoT systems. Because of the neglected and distributed nature of the IoT systems, most IoT devices usually work in open-air environments that are incredibly susceptible to physical attacks [46].

2. **Reconnaissance attacks:** The illegal discovery and mapping of systems and services are mainly involved in reconnaissance attacks. Scanning network ports, traffic analysis, packet sniffers, and sending queries about Internet Protocol (IP) address information are some examples of reconnaissance attacks [46].

3. **Denial-of-service (DoS):** The cyber attacker performs the DoS attack to make a system, or network resource inaccessible to the target users, which is the primary goal of the DoS attack. Most IoT and embedded devices are highly vulnerable to resource enervation attacks due to average or low-level memory capabilities and minimal computation resources [46].

4. **Access attacks:** These attacks involve unofficial persons gain access to networks or systems to which they have no legal access. The two different access attacks are physical access and remote access. In physical access, the attacker can gain access to a device physically. In remote access, the offender attacks the (Internet Protocol) IP-connected devices [46].

5. **Attacks on privacy:** Since large volumes of information are easily reachable over remote access mechanisms, privacy protection in IoT has become highly challenging. The most well-known attacks on user privacy are data mining, cyber espionage, tracking, and eavesdropping [46].

6. **Firmware hijacking:** The firmware updates downloaded by an IoT device from a non-legitimate source increase the system vulnerabilities and helps the cyber attacker to hijack the device and download malicious software. Malware and Trojan Horse involve in this kind of attack. So, the user must make sure the firmware updates got downloaded from the official website [47].

7. **Password-based attacks:** Password-based attacks are more common than other cyber-attacks on IoT devices. In this kind of attack; Intruders attempt to generate a valid duplicate user password. The IoT devices with weak or average strength passwords are highly susceptible to this attack. The password-based attack mainly occurs in two different ways: dictionary attacks and brute force attacks [46].

The businesses that could not detect whether their IoT systems are attacked or infected by a virus are 48%. Almost 41% of industries are not encrypting all of their data, and 35% of the business organizations do not have cyber security analyst or engineer who helps to prevent the attacks in advance and take respective countermeasures in case of live cyber-attacks [104].

The Attacks on the TCP/IP layers of the Embedded Systems :

The TCP/IP model includes the application, transport, network, link, and physical layers. The embedded systems are generally located at the physical layer of IoT systems which is the bottom layer. Security threats may typically occur at the upper layers of the TCP/IP model, and during the design phase of embedded systems, most direct threats occur at the physical layer [3]. Figure 5 outlines the classic cyber-attacks on the TCP/IP layers.

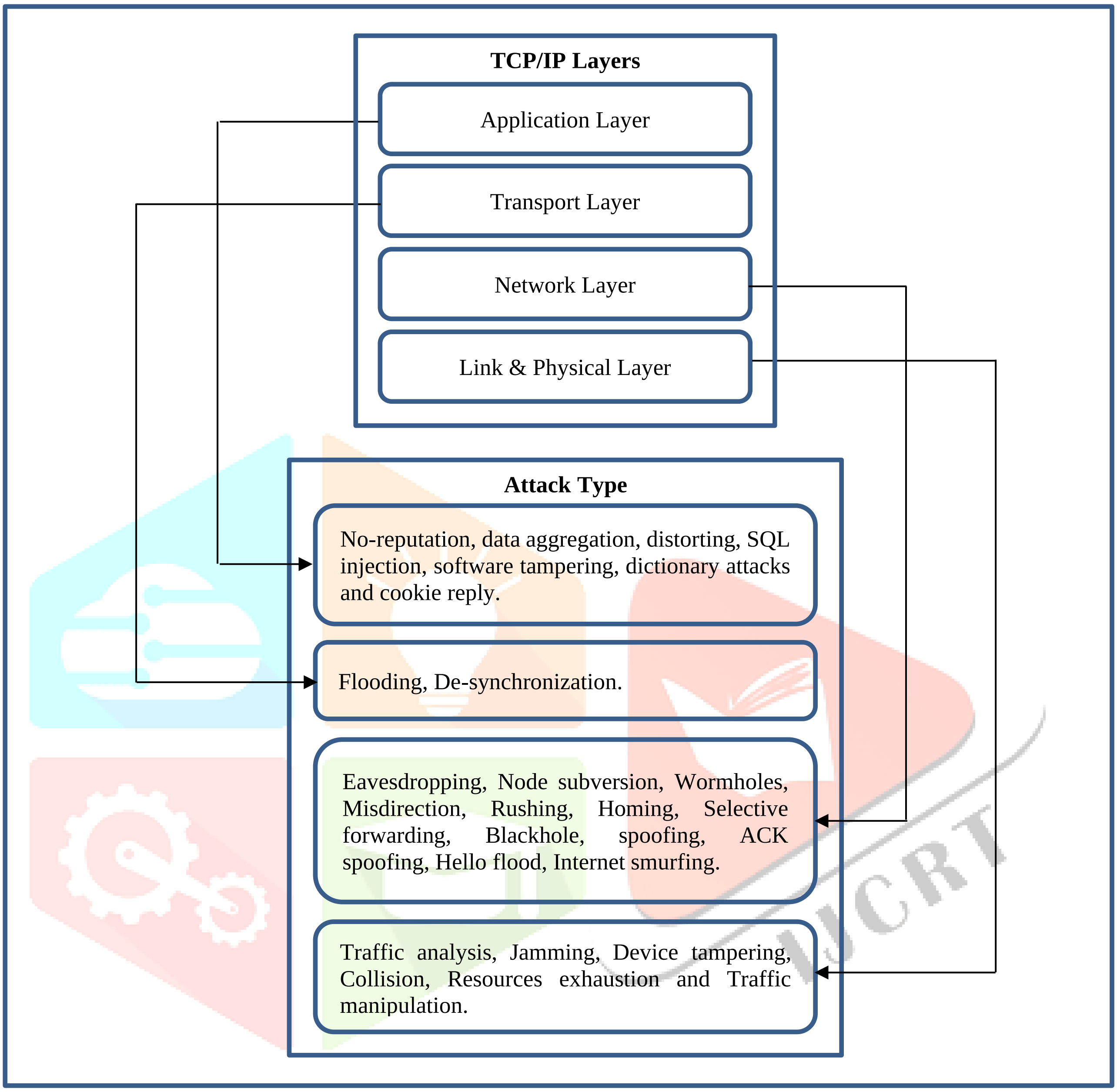
TCP/IP Layers
Application Layer
Transport Layer
Network Layer
Link & Physical Layer
Attack Type
No-reputation, data aggregation, distorting, SQL injection, software tampering, dictionary attacks and cookie reply.
Flooding, De-synchronization.
Eavesdropping, Node subversion, Wormholes, Misdirection, Rushing, Homing, Selective forwarding, Blackhole, spoofing, ACK spoofing, Hello flood, Internet smurfing.
Traffic analysis, Jamming, Device tampering, Collision, Resources exhaustion and Traffic manipulation.

Figure 5: TCP/IP Layers and Attacks [3], [37].

Prevention of cyberattacks is so hard for an embedded system engineer because of the variety of attacks and the various constraints present in the embedded systems. Detection of the attack is one of the most critical stages in dealing with a cyberattack in the embedded system. Detection of an attack after some time could allow terrible consequences, like system damage, to occur, whereas immediate detection allows for a suitable response. However, detection may require significant resources and limit the functionality of the embedded system. Improper response could contribute to an attack and even be used by an attacker [3].

Most of the cyberattacks in embedded and IoT systems are due to human errors. For example, lousy user habits as using a weak or default username and password from the manufacturer for their IoT devices could lead to penetration of the system's security easily with the help of a botnet. A group of internet-connected devices infected by malware that allows cyber attackers to control them and attack against the target user or system is known as the botnet. Botnets are used in large numbers to instigate botnet attacks by cyber attackers, including DDoS attacks, unauthorized access to the system, user credentials/data leaks, and other malicious activities [6]. The rate of successful cyberattacks on IoT devices has increased tremendously over the past years. Figure 6 displays the global distribution of cyberattacks on IoT devices all around the world.

In 2020, Nokia threat intelligence reports that infected IoT devices jumped from 16.17% in 2019 to 32.72% in 2020 [106]. The trojan is the malware that caused enormous cyberattacks in 2020. The spread of trojan malware jumped from 34% in 2019 to 74% in 2020 [106]. The availability of IoT botnets for rent massively increases DDoS attacks. At a price of just $0.35, a person can rent an HTTP DDoS botnet for 10 minutes to organize a DDoS attack against a target user or system [107].

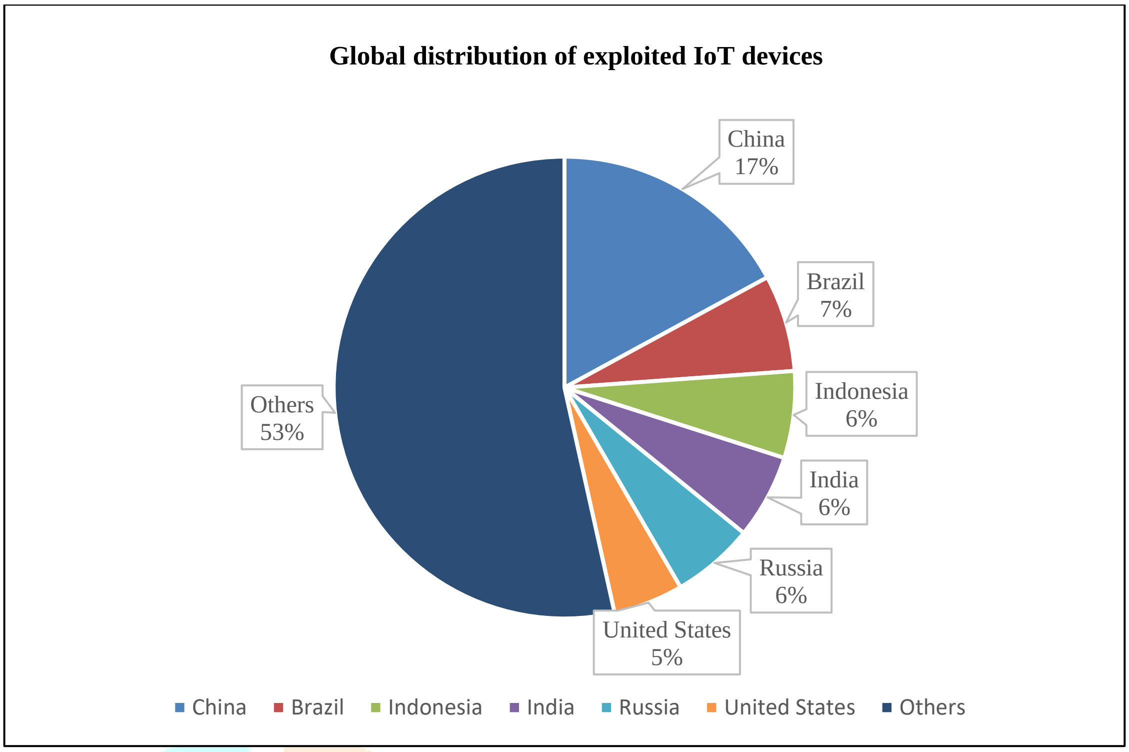

Figure 6: Global distribution of exploited IoT devices [48], [49].

According to the security threat intelligence report released by NETSCOUT for the second half of 2018, IoT devices are getting attacked by various cyber attackers when connected to the internet. Most of the IoT devices are getting stormed every five minutes by enormous attackers in cyberspace [107]. The report released by Palo Alto Networks in 2020 states that out of 100%, almost 83% of diagnostic medical imaging equipment is running on outdated operating systems (OS). It also describes the unencrypted IoT system traffic as nearly 98%, which exposes all kinds of highly sensitive or confidential data of a user or user on the network [107].

IV. COUNTERMEASURES

Countermeasures must make sure that it ensures the CIA triad at any cost. The hindrance in implementing the countermeasure is because of the constraints tied with the embedded systems. Those constraints are battery, processing power, and system memory [24]. The cost and life of batteries thwart the embedded system from implementing high-end crypto algorithms and firewalls [50]. Hence, the attackers find it very easy to exploit by brute force. Device misconfiguration may affect the system's integrity. The firmware of the embedded system should only be updated from an official website and appropriately patched. Protocols must implement the safety of the systems on their own rather than requiring to be forced. Table I displays the countermeasures for various attacks on the embedded systems [24].

Table I – Countermeasures for cyberattacks on Embedded systems [24].

Attack	Category	Countermeasures
Malware	Software-based attack	Anti-malware application [51], Machine-learning-based application [52].
Brute Force	Software-based attack	Limiting the number of tries
Buffer overflow	Software-based attack	Hardware/Software Defender technique [53].
Web-based vulnerability	Software-based attack	Sandboxing [54].
MITM	Network-based attack	IPsec [55].
DNS poisoning	Network-based attack	DNSSEC [56].
Session hijacking	Network-based attack	Encryption, disposable credits [57].
Signal jamming	Network-based attack	Anti-jamming mechanism [58].
Power analysis	Physical and side-channel based attacks	Data Masking technique [66].
Timing attacks	Physical and side-channel based attacks	Random clock technique [60].
Electromagnetic analysis attack	Physical and side-channel based attacks	Shielding techniques [61], Asynchronism [61].

The massive development in the field of IoT systems and Industrial IoT (IIoT) systems has brought enormous demand for smart electronic devices like sensors and other equipment that can sense information from the environment, process and transmit it to the destined locations for further analysis and conclusions. Due to this extreme demand, the manufacturers compromise the security features of the various IoT systems [64]. Therefore, both commercial and industrial-oriented IoT devices are highly vulnerable to multiple types of cyberattacks. So, it is necessary to follow some measures to prevent IoT systems from cyberattacks [65].

To consistently provide an authentic connection between entities and a proper authentication mechanism together with confidentiality about data is the security objective of the IoT system. This objective leads to the information security or CIA triad that offers confidentiality, integrity, and availability of the data. A thread in any one of these essential areas could cause severe harm to the system and have the worst impact on the function of the system [62].

Table II – CIA Security Model [62].

CIA SECURITY MODEL	
Confidentiality	Unauthorized access is prevented.
Integrity	Data cannot be modified.
Availability	Data cannot be unavailable.

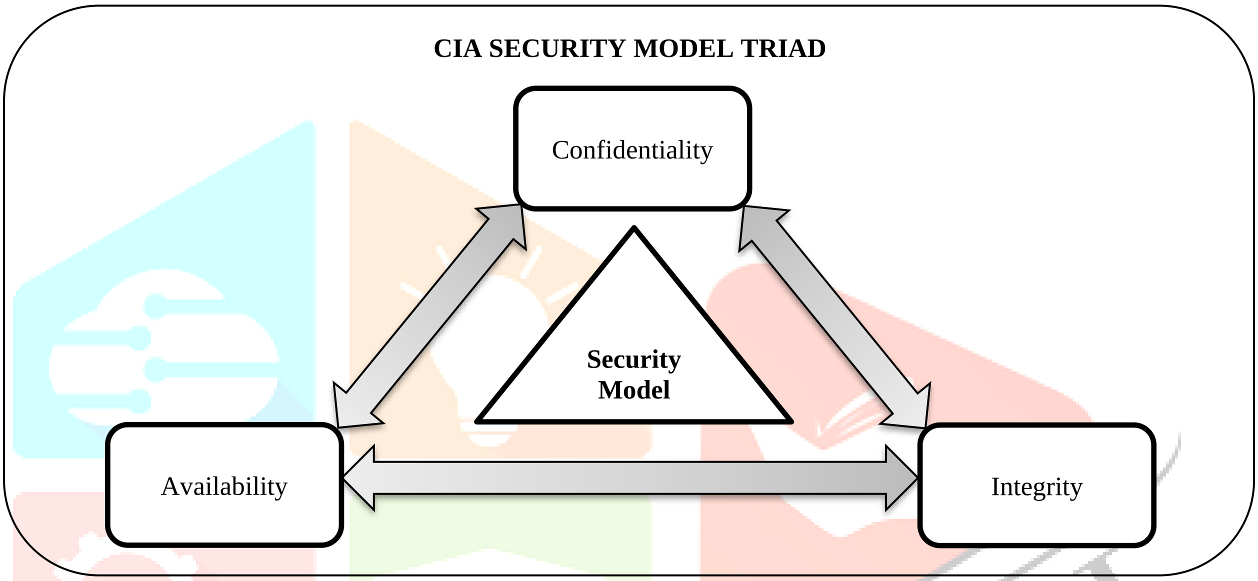

Figure 7: CIA Security Model [62].

i. **Data Confidentiality** refers to the potential to provide and assure privacy for highly sensitive data and the user's information. The confidentiality of the data can be attained through encryption of the data like Triple-DES, AES, RSA Security, blowfish, ciphertext, and many other encryption algorithms [63]. Data Confidentiality in the IoT system prevents the IoT devices from connecting and transmitting data to an unauthorized server or entity [62].

ii. **Data Integrity** refers to the ability to secure sensitive data and information from attackers during the communication or transmission of data. The consistency, accuracy, and trustworthiness of data are maintained by the integrity till the existence of data. Checksum and cyclic redundancy are two methods that are used for checking data integrity [62].

iii. **Data Availability** is the final and important component of the CIA security model. It intends to provide data for users whenever they needed. The data can be accessed by the users during any conditions, which include disastrous and normal conditions. The DoS attack could deny data availability. So activating firewalls in the network helps to block the DoS attack. The other mechanisms like IDS and redundancy methods help to protect data availability [62].

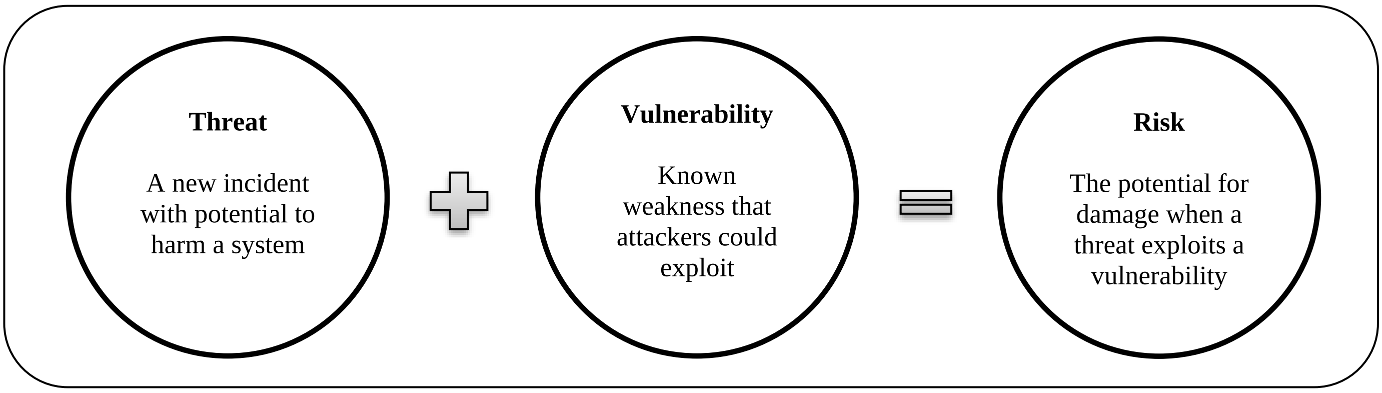
Threat
A new incident with potential to harm a system
Vulnerability
Known weakness that attackers could exploit
Risk
The potential for damage when a threat exploits a vulnerability

Figure 8: The Rise of Risk [108].

Through implementing preventive measures, users could limit various cyberattacks on both embedded and IoT systems. By executing countermeasures, users could minimise the damage of cyberattacks.

Table III – Countermeasures for cyberattacks on IoT systems [6].

Attack	Target Layer	Countermeasures
Eavesdropping	All layers	Link-layer encryption [66], [67], [68], [69], [70], [71], SensorWare communication multicast model [72], Key pre-distribution [73], [74], [75]
Tampering	Physical Layer	Tamper resistant hardware, disabling JTAG and/or protecting bootstrap loader [76], camouflaging [77]
HELLO flooding	Network Layer	Identity verification protocol [66], Multi-path multi-base station routing [78], μ-TESLA [67]
Node-Replication (Clone)	Network Layer	ID-based public keys [79], Location-based key management [80], Multi-level clustering [81]
Blackhole	Network Layer	REWARD routing [82], Multi-path routing [66], [83], [84], Mesh network topology [85], ActiveTrust routing [86], Isolation [87], BAMBi [88], MAODV [89]
Sybil	Network Layer	Indirect validation [66], Identity verification [90], Isolation [91], ID-based public keys [79]
Selective forwarding (Grayhole)	Network Layer	Multi-path routing [66], [84], Usage of source authorization [83]
Sinkhole	Network Layer	Secure routing algorithm [92]
Wormhole	Network Layer	Location-based keys [79], Centralized computing [93], DAWWSEN [94]
Session hijacking	Transport Layer	Light-weight user authentication algorithm for optimized routing in mobile networks [95]
MQTT exploit	Transport Layer	Enforcement of security policies [96], SMQTT [97]
SYN-flooding	Transport Layer	SYN-cookies [98], Client puzzles [99]
De-Synchronization	Transport Layer	Usage of authentication including transport layer protocol headers [100]
False data injection	Application Layer	Collective secret [101]
CoAP exploit	Application Layer	CoAPs, employment of DTLS [102]
Path-based DoS	Application Layer	One-way hash chains [103]

V. Conclusion

The Embedded and IoT systems have made almost everyone's life very convenient and comfortable. In this paper, the significant vulnerabilities present in both embedded and IoT systems and their countermeasures are scrutinized. Both Embedded and IoT systems are large-scale, complex architectural designs comprising a variety of heterogeneous devices. Therefore, scalability, transparency, and reliability are the most conspicuous issues to be solved immediately. System security-related initiatives need to consider these issues primarily. Moreover, Manufacturers should ensure high-level security features in both higher and lower-level system architectural security design. These security features can accomplish this by designing lightweight security protocols, and cryptography algorithms customized based on the precise needs of the resource-constrained devices of embedded and IoT systems.

This paper concludes that extensive work remains to be done in the security area of embedded and IoT systems by both manufacturers and end-users. End end-users should scan the system regularly to detect any new vulnerabilities and take countermeasures at the right time. The aim is to achieve a better and deeper understanding of the security threats facing IoT infrastructure and identify the likelihood and consequences of threats to IoT systems in future works. This paper discussed the overall trend in the security of embedded and IoT systems. However, embedded and IoT systems' heterogeneous nature and restrictions will make any resolution inappropriate and obsolete. Furthermore, it is expected that security researchers will reveal many more vulnerabilities and countermeasures soon because of the dynamic nature of technology.

REFERENCES

[1]. K.V. Shibu (2017) *Introduction to Embedded Systems*, Second edn., : McGraw Hill Education India Private Limited.

[2]. Anjana Bose (2018) *Embedded System – Characteristics, Types, Advantages & Disadvantages*, Available at: *https://electricalfundablog.com/embedded-system-characteristics-types-advantages-disadvantages/*

[3]. A. Aloseel, H. He, C. Shaw and M. A. Khan, "Analytical Review of Cybersecurity for Embedded Systems," in IEEE Access, vol. 9, pp. 961-982, 2021, doi: 10.1109/ACCESS.2020.3045972.

[4]. Sudip Misra, Chandana Roy and Anandarup Mukherjee (2021) *Introduction to Industrial Internet of Tings and Industry 4.0*, First edn., : CRC Press.

[5]. Sita Rani, Aman Kataria, Vishal Sharma, Smarajit Ghosh, Vinod Karar, Kyungroul Lee, Chang Choi, "Threats and Corrective Measures for IoT Security with Observance of Cybercrime: A Survey", *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 5579148, 30 pages, 2021. https://doi.org/10.1155/2021/5579148

[6]. I. Butun, P. Osterberg, and H. Song, "Security of the internet of things: vulnerabilities, attacks, and countermeasures," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 616–644, 2020.

[7]. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: architecture, enabling technologies, security, and privacy, and applications," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, 2017..

[8]. S. Jeschke, C. Brecher, H. Song, and D. Rawat, Industrial Internet of Things: Foundations, Principles and Applications, Springer, Cham, Switzerland, 2017.

[9]. H. Song, D. B. Rawat, S. Jeschke, and C. Brecher, Cyber-physical Systems: Foundations, Principles and Applications, Morgan Kaufmann, 2016.

[10]. P. V. Astillo, J. Kim, V. Sharma, and I. You, "SGF-MD: behavior rule specification-based distributed misbehavior detection of embedded IoT devices in a closed-loop smart greenhouse farming system," IEEE Access, vol. 8, pp. 196235–196252, 2020.

[11]. A. Kataria, S. Ghosh, V. Karar, T. Gupta, K. Srinivasan, and Y.-C. Hu, "Improved diver communication system by combining optical and electromagnetic trackers," Sensors, vol. 20, no. 18, p. 5084, 2020.

[12]. V. Sharma, R. Kumar, and R. Kaur, "UAV-assisted content based sensor search in IoTs," Electronics Letters, vol. 53, no. 11, pp. 724–726, 2017.

[13]. I. You, H.-C. Chen, V. Sharma, and I. Kotenko, Mobile Internet Security: Second International Symposium, MobiSec 2017, vol. 971, Springer, Jeju Island, Republic of Korea, 2018, October 19–22, 2017, Revised Selected Papers.

[14]. H. G. Brauch, "Concepts of security threats, challenges, vulnerabilities and risks," in Coping with Global Environmental Change, Disasters and Security. Springer, 2011, pp. 61–106.

[15]. K. Dahbur, B. Mohammad, and A. B. Tarakji, "A survey of risks, threats, and vulnerabilities in cloud computing," in Proceedings of the 2011 International conference on intelligent semantic Web-services and applications. ACM, 2011, p. 12.

[16]. R. K. Rainer and C. G. Cegielski, Introduction to information systems: Enabling and transforming business. JohnWiley & Sons, 2010.

[17]. A. J. Duncan, S. Creese, and M. Goldsmith, "Insider attacks in cloud computing," in Trust, Security, and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012, pp. 857–862.

[18]. P. Baybutt, "Assessing risks from threats to process plants: Threat and vulnerability analysis," Process Safety Progress, vol. 21, no. 4, pp. 269–275, 2002.

[19]. C. Tankard, "Advanced persistent threats and how to monitor and deter them," Network Security, vol. 2011, no. 8, pp. 16–19, 2011.

[20]. F. Li, A. Lai, and D. Ddl, "Evidence of advanced persistent threat: A case study of malware for political espionage," in Malicious and Unwanted Software (MALWARE), 2011 6th International Conference on. IEEE, 2011, pp. 102–109.

[21]. P. Koopman, "Embedded System Security," Computer (Long. Beach. Calif)., no. July, pp. 95–97, 2004.

[22]. C. O'Flynn and Z. Chen, "ChipWhisperer: An Open-Source Platform for Hardware Embedded Security Research," 2014, pp. 243–260.

[23]. Riya Savjani (2018) *6 Critical Challenges Facing the Embedded Systems Security* , Available at: *https://www.einfochips.com/blog/6-critical-challenges-facing-the-embedded-systems-security/*

[24]. Rajendran, Gowthamaraj and Nivash, Ragul, Security in the Embedded System: Attacks and Countermeasures (July 31, 2019). Proceedings of International Conference on Recent Trends in Computing, Communication & Networking Technologies (ICRTCCNT) 2019, Available at SSRN: https://ssrn.com/abstract=3429857 or http://dx.doi.org/10.2139/ssrn.3429857

[25]. Alina Beliba (2020) *12 common attacks on embedded systems and how to prevent them*, Available at: *https://www.apriorit.com/dev-blog/690-embedded-systems-attacks*

[26]. Cui, Ang, Michael Costello, and Salvatore Stolfo. "When firmware modifications attack: A case study of embedded exploitation." (2013).

[27]. Owens, Jim, and Jeanna Matthews. "A study of passwords and methods used in brute-force SSH attacks." USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET). 2008.

[28]. Riihijarvi, Janne, et al. "Providing network connectivity for small appliances: a functionally minimized embedded Web server." IEEE Communications Magazine 39.10 (2001): 74-79.

[29]. Man-in-the-Middle Attack (MITM). (2017, March 30). Techopedia.Com. https://www.techopedia.com/definition/4018/man-in-the-middle-attack-mitm

[30]. DNS Cache Poisoning - The Next Generation. (2011, March 3). Secureworks. https://www.secureworks.com/blog/dns-cache-poisoning

[31]. Ben Lutkevich, & Kevin Beaver. (2021, June 3). distributed denial-of-service (DDoS) attack. SearchSecurity. https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack

[32]. Session hijacking attack Software Attack | OWASP Foundation. (n.d.). OWASP Foundation. Retrieved June 17, 2021, from https://owasp.org/www-community/attacks/Session_hijacking_attack

[33]. Reade, Walter C., Daniel L. Ellingson, and Jeff Lindsay. "Jamming device against RFID smart tag systems." U.S. Patent No. 7,221,900. 22 May 2007.

[34]. Brier, Eric, Christophe Clavier, and Francis Olivier. "Correlation power analysis with a leakage model." International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2004.

[35]. Kocher, Paul, et al. "Security as a new dimension in embedded system design." Proceedings of the 41st annual Design Automation Conference. ACM, 2004.

[36]. Chari, Suresh, Josyula R. Rao, and Pankaj Rohatgi. "Template attacks." International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2002.

[37]. S. Ali, T. Al Balushi, Z. Nadir, and O. K. Hussain, ICS/SCADA system security for CPS, vol. 768. 2018.

[38]. A. Venčkauskas, R. Damaševičius, V. Jusas, J. Toldinas, D. Rudzika, and G. Drėgvaitė, "A review of cyber-crime in internet of things: technologies, investigation methods and digital forensics," International Journal of Engineering Sciences and Research Technology, vol. 4, pp. 460–477, 2015.

[39]. I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. M. A. Kazmi, and C. S. Hong, "Internet of things forensics: recent advances, taxonomy, requirements, and open challenges," Future Generation Computer Systems, vol. 92, pp. 265–275, 2019.

[40]. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," IEEE Access, vol. 7, pp. 82721–82743, 2019.

[41]. P. Radanliev, D. C. de Roure, R. Nicolescu et al., "Future developments in cyber risk assessment for the internet of things," Computers in Industry, vol. 102, pp. 14–22, 2018.

[42]. N. H. N. Zulkipli, A. Alenezi, and G. B. Wills, "IoT forensic: bridging the challenges in digital forensic and the internet of things," in Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, pp. 315–324, Porto, Portugal, 2017.

[43]. M. Husamuddin and M. Qayyum, "Internet of things: a study on security and privacy threats," in 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), pp. 93–97, Abha, 2017.

[44]. Gloss, K. (2020, October 8). 5 IoT security threats to prioritize. IoT Agenda. https://internetofthingsagenda.techtarget.com/tip/5-IoT-security-threats-to-prioritize

[45]. Aamir Lakhani. (2021, June 7). Examining Top IoT Security Threats and Attack Vectors | Fortinet. Fortinet Blog. https://www.fortinet.com/blog/industry-trends/examining-top-iot-security-threats-and-attack-vectors

[46]. Abomhara, M., & Koien, G. M. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security and Mobility, 4(1), 65–88. https://doi.org/10.13052/jcsm2245-1439.414

[47]. Garey, L. (2018, July 16). IoT Insecurity: 6 Common Attacks and How to Protect Customers. Channel Futures. https://www.channelfutures.com/best-practices/iot-insecurity-6-common-attacks-and-how-to-protect-customers

[48]. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale iot exploitations. IEEE Commun. Surv. Tutor. 2019, 21, 2702–2733.

[49]. Anand, P.; Singh, Y.; Selwal, A.; Singh, P.K.; Felseghi, R.A.; Raboaca, M.S. IoVT: Internet of Vulnerable Things? Threat Architecture, Attack Surfaces, and Vulnerabilities in Internet of Things and Its Applications towards Smart Grids. Energies 2020, 13, 4813. https://doi.org/10.3390/en13184813.

[50]. Baheti, Radhakisan, and Helen Gill. "Cyber-physical systems." The impact of control technology 12.1 (2011): 161-166

[51]. Peikari, Cyrus. "Protection of embedded processing systems with a configurable, integrated, embedded firewall." U.S. Patent Application No. 10/346,956.

[52]. Sayadi, Hossein, et al. "Customized machine learning-based hardware-assisted malware detection in embedded devices." 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, 2018.

[53]. Shao, Zili, et al. "Security protection and checking for embedded system integration against buffer overflow attacks via hardware/software." IEEE Transactions on Computers 55.4 (2006): 443-453.

[54]. Bak, Stanley, et al. "Sandboxing controllers for cyber-physical systems." 2011 IEEE/ACM Second International Conference on Cyber-Physical Systems. IEEE, 2011.

[55]. "IPsec-Internet-Protocol-Security." [Online] Available:https://searchsecurity.techtarget.com/definition/IPsec-Internet-Protocol-Security

[56]. "dnssec-what-is-it-why-important" [Online]. Available:https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en

[57]. Dacosta, Italo, et al. One-time cookies: Preventing session hijacking attacks with disposable credentials. Georgia Institute of Technology, 2011.

[58]. Pajic, Miroslav, and Rahul Mangharam. "Anti-jamming for embedded wireless networks." 2009 International Conference on Information Processing in Sensor Networks. IEEE, 2009.

[59]. Shu, David B., Lap-Wai Chow, and William M. Clark Jr. "Cryptographic architecture with random instruction masking to thwart differential power analysis." U.S. Patent No. 8,065,532. 22 Nov. 2011.

[60]. Ravi, Srivaths, Anand Raghunathan, and Srimat Chakradhar. "Tamper resistance mechanisms for secure embedded systems." 17th International Conference on VLSI Design. Proceedings. IEEE, 2004.

[61]. Quisquater, Jean-Jacques, and David Samyde. "Electromagnetic analysis (ema): Measures and counter-measures for smart cards." International Conference on Research in Smart Cards. Springer, Berlin, Heidelberg, 2001.

[62]. Security in IoT - Security solution for IoT communication protocol. (2019, May 26). Cryptiot. https://cryptiot.de/iot/security/security-solution-iot-com-protocol/

[63]. 5 Common Encryption Algorithms and the Unbreakables of the Future. (2021, June 22). StorageCraft Technology, LLC. https://blog.storagecraft.com/5-common-encryption-algorithms/

[64]. S. Li and L. Da Xu, Securing the internet of things. Syngress, 2017.

[65]. J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial iot devices," in Design Automation Conference (ASP-DAC), 2016 21st Asia and South Pacific.IEEE, 2016, pp. 519–524.

[66]. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad hoc networks, vol. 1, no. 2, pp. 293–315, 2003.

[67]. A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "Spins: Security protocols for sensor networks,"Wireless networks, vol. 8, no. 5, pp. 521–534, 2002.

[68]. J. Deng, R. Han, and S. Mishra, "A performance evaluation of intrusion-tolerant routing in wireless sensor networks," in Information Processing in Sensor Networks. Springer, 2003, pp. 552–552.

[69]. R. Di Pietro, L. V. Mancini, Y. W. Law, S. Etalle, and P. Havinga, "Lkhw: A directed diffusion-based secure multicast scheme for wireless sensor networks," in Parallel Processing Workshops, 2003. Proceedings. 2003 International Conference on. IEEE, 2003, pp. 397–406.

[70]. M. Tubaishat, J. Yin, B. Panja, and S. Madria, "A secure hierarchical model for sensor network," ACM Sigmod Record, vol. 33, no. 1, pp. 7–13, 2004.

[71]. C. Karlof, N. Sastry, and D.Wagner, "Tinysec: a link layer security architecture for wireless sensor networks," in Proceedings of the 2nd international conference on Embedded networked sensor systems. ACM, 2004, pp. 162–175.

[72]. S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, and M. B. Srivastava, "On communication security in wireless ad-hoc sensor networks," in Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshops on. IEEE, 2002, pp. 139–144.

[73]. W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," ACM Transactions on Information and System Security (TISSEC), vol. 8, no. 2, pp. 228–258, 2005.

[74]. H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Security and Privacy, 2003. Proceedings. 2003 Symposium on. IEEE, 2003, pp. 197–213.

[75]. L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proceedings of the 9th ACM Conference on Computer and Communications Security. ACM, 2002, pp. 41-47.

[76]. W. Znaidi, M. Minier, and J.-P. Babau, "An ontology for attacks in wireless sensor networks," Ph.D. dissertation, INRIA, 2008.

[77]. K. Sharma and M. Ghose, "Wireless sensor networks: An overview on its security threats," IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs, pp. 42–45, 2010.

[78]. M. A. Hamid, M. Rashid, and C. S. Hong, "Routing security in sensor network: Hello flood attack and defense," IEEE ICNEWS, pp. 2–4, 2006.

[79]. Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks," IEEE Journal on selected areas in communications, vol. 24, no. 2, pp. 247–260, 2006.

[80]. M.-j. Duan and J. Xu, "An efficient location-based compromise-tolerant key management scheme for sensor networks," Information Processing Letters, vol. 111, no. 11, pp. 503–507, 2011.

[81]. I. Butun, I.-H. Ra, and R. Sankar, "An intrusion detection system based on multi-level clustering for hierarchical wireless sensor networks," Sensors, vol. 15, no. 11, pp. 28 960–28 978, 2015.

[82]. Z. Karakehayov, "Using reward to detect team black-hole attacks in wireless sensor networks," Wksp. Real World Wireless Sensor Networks, pp. 20–21, 2005.

[83]. A. Agah and S. K. Das, "Preventing dos attacks in wireless sensor networks: A repeated game theory approach." IJ Network Security, vol. 5, no. 2, pp. 145–153, 2007.

[84]. D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highlyresilient, energy-efficient multipath routing in wireless sensor networks," ACM SIGMOBILE Mobile Computing and Communications Review, vol. 5, no. 4, pp. 11–25, 2001.

[85]. S. N. Krishnan and P. Srinivasan, "A qos parameter based solution for black hole denial of service attack in wireless sensor networks," Indian Journal of Science and Technology, vol. 9, no. 38, 2016.

[86]. Y. Liu, M. Dong, K. Ota, and A. Liu, "Activetrust: secure and trustable routing in wireless sensor networks," IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 2013–2027, 2016.

[87]. M. Wazid, A. Katal, R. S. Sachan, R. Goudar, and D. Singh, "Detection and prevention mechanism for blackhole attack in wireless sensor network," in Communications and Signal Processing (ICCSP), 2013 International Conference on. IEEE, 2013, pp. 576–581.

[88]. S. Misra, K. Bhattarai, and G. Xue, "Bambi: Blackhole attacks mitigation with multiple base stations in wireless sensor networks," in Communications (ICC), International Conference on. IEEE, 2011, pp. 1–5.

[89]. M. Medadian, M. H. Yektaie, and A. M. Rahmani, "Combat with black hole attack in aodv routing protocol in manet," in Internet, 2009. AH-ICI 2009. First Asian Himalayas International Conference on. IEEE, 2009, pp. 1–5.

[90]. J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in Proceedings of the 3rd international symposium on Information processing in sensor networks. ACM, 2004, pp. 259–268.

[91]. P. Sarigiannidis, E. Karapistoli, and A. A. Economides, "Detecting sybil attacks in wireless sensor networks using uwb rangingbased information," Expert Systems with Applications, vol. 42, no. 21, pp. 7560–7572, 2015.

[92]. L. Teng and Y. Zhang, "Sera: a secure routing algorithm against sinkhole attacks for mobile wireless sensor networks," in Computer Modeling and Simulation, 2010. ICCMS'10. Second International Conference on, vol. 4. IEEE, 2010, pp. 79–82.

[93]. W.Wang and B. Bhargava, "Visualization of wormholes in sensor networks," in Proceedings of the 3rd ACM workshop on Wireless security. ACM, 2004, pp. 51–60.

[94]. R. Z. El Kaissi, A. Kayssi, A. Chehab, and Z. Dawy, "Dawwsen: A defense mechanism against wormhole attacks in wireless sensor networks," Ph.D. dissertation, American University of Beirut, Department of Electrical and Computer Engineering, 2005.

[95]. S. Song, H.-K. Choi, and J.-Y. Kim, "A secure and lightweight approach for routing optimization in mobile ipv6," EURASIP Journal on Wireless Communications and Networking, vol. 2009, p. 7, 2009.

[96]. R. Neisse, G. Steri, and G. Baldini, "Enforcement of security policy rules for the internet of things," in Wireless and Mobile Computing, Networking and Communications (WiMob), 2014 IEEE 10th International Conference on. IEEE, 2014, pp. 165–172.

[97]. M. Singh, M. Rajan, V. Shivraj, and P. Balamuralidhar, "Secure mqtt for internet of things (iot)," in Communication systems and network technologies (CSNT), 2015 fifth international conference on. IEEE, 2015, pp. 746–751.

[98]. D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," IEEE Pervasive Computing, vol. 7, no. 1, 2008.

[99]. T. Aura, P. Nikander, and J. Leiwo, "Dos-resistant authentication with client puzzles," in International workshop on security protocols. Springer, 2000, pp. 170–177.

[100]. A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," Computer, vol. 35, no. 10, pp. 54–62, 2002.

[101]. F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," IEEE Journal on Selected Areas in Communications, vol. 23, no. 4, pp. 839–850, 2005.

[102]. R. A. Rahman and B. Shah, "Security analysis of iot protocols: A focus in coap," in Big Data and Smart City (ICBDSC), 2016 3rd MEC International Conference on. IEEE, 2016, pp. 1–7.

[103]. J. Deng, R. Han, and S. Mishra, "Defending against path-based dos attacks in wireless sensor networks," in Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks. ACM, 2005, pp. 89–96.

[104]. 10 Must-Know IoT Cybersecurity Stats | BehrTech Blog. (2021, May 11). BehrTech. https://behrtech.com/blog/infographic-10-must-know-iot-cybersecurity-stats/

[105]. Micke Ahola. (n.d.). The Role of Human Error in Successful Cyber Security Breaches. Usecure. https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches

[106]. Infected IoT device numbers grow 100% in a year. (2020b, October 26). Security Magazine. https://www.securitymagazine.com/articles/93731-infected-iot-device-numbers-grow-100-in-a-year

[107]. Crane, C. (2021, April 21). Re-Hashed: 27 Surprising IoT Statistics You Don't Already Know. Hashed Out by The SSL StoreTM. https://www.thesslstore.com/blog/20-surprising-iot-statistics-you-dont-already-know/

[108]. Kidd, C. (n.d.). What Is the CIA Security Triad? Confidentiality, Integrity, Availability Explained. BMC Blogs. https://www.bmc.com/blogs/cia-security-triad/