An Analysis of Security Risk Factors in IoT and Defensive Measures to Mitigate Data Breaches

Thivanka Mohottalalage[a] and Akalanka Mailewa[b]

[a]Department of Information Systems, St. Cloud State University, St. Cloud, MN, United States

[b]Department of Computer Science and Information Technology, St. Cloud State University, St. Cloud, MN, United States

Abstract

The Internet of Things' (IoT) quick development and user-friendly features have drawn interest from every industry to help them with their everyday operations. The world is being shaped by the expansion of IoT in ways that will improve efficiency, productivity, development, and opportunity while also raising quality of life. But the speed at which information technology is developing and progressing has become addictive, and as we struggle to create laws, regulations, and governance that influence this development without stifling innovation, our security and liberties are coming under more and more threat from the lack of security knowledge of the application. Security risks have made it possible to improve business operations while decreasing everyday production, sales, and customer service efficiency. Unauthorized access sets off hostile activity, causing data to lose its integrity and having a catastrophic impact on the company's day-to-day operations. The significance of IoT, its architecture, some of its main application areas, as well as its security and privacy challenges, are covered in this article. It will highlight some of the most significant technological advancements and provide an overview of a few applications that could significantly impact people's lives. This article also highlights the fact that logical defects in embedded binaries are the specificity of vulnerability detection in IoT firmware.

Keywords: IoT, Security, Policy, Detection, Prevention, Attacks, Sensor Networks

1. Introduction

The internet has become pervasive in today's society, impacting nearly every region of the planet and having incalculable effects on human existence. The era of the "Internet of Things" has begun. The term "Internet of Things" (IoT) describes a scenario in which practically every item and gadget we use is networked [1]. The growth of the internet of things is hailed as having the potential to drastically alter our way of life. It is acknowledged as an enabler that will boost productivity in a number of fields, such as manufacturing, logistics, and transportation [2]. The Internet of Things will leverage sophisticated data to help optimize processes through advanced data analytics and, by leveraging its cyber-physical properties, be the impetus for new market segments and the emergence of cross-cutting services and applications. Applications of the internet of things will affect practically every aspect of our lives, not only the nation's economy. Since maintaining database records is essential to the smooth running of any business, data protection is the key to many safe systems in any corporation [3][4].

IoT security aims to shield databases against unintentional or deliberate loss. These hazards to the data's dependability and integrity. The Internet of Things (IoT) refers to the process of connecting items or things to the network so they can exchange and gather data with one another as well as via the network. The Internet of Things has numerous fascinating uses and has advanced several industries, including healthcare, transportation, and agriculture. The Internet of Things (IoT) has brought about a significant digital transition in the way people, homes, and companies interact on a daily basis. However, in addition to creating engaging applications, it's important to take into account other aspects including data storage, security, and privacy [1][2][5]. People are becoming more aware of their surroundings with devices such as smoke detectors, alarm systems, refrigerators, thermostats, and effective water supply and transportation management. Every industry has access to IoT applications, including retail, agriculture, travel and personal care, healthcare, construction, smart homes, and retail. IoT is centered on automation and logistics, particularly in the industrial sector, to produce smarter solutions that adapt to human behavior [6][7]. IOT has the potential to impact almost every aspect of the economy; its devices will range in size and shape from nanochips to smart device machines. Globally, there will be a significant surge in linked IoT devices, with estimates reaching 125 billion by 2030 [8]. The overview of IoT is separated into two parts:

1.1. IoT Architecture

Figure 1.A depicts the most basic architecture, which is a three-layer architecture which has the application, network, and perception layers [1][2][3].

- The physical layer, or perception layer, is equipped with sensors to sense and collect environmental data. It recognizes other intelligent items in the surroundings and senses a few physical characteristics.
- The network layer is in charge of sending and processing sensor data as well as establishing connections with other smart objects, servers, and network devices.
- Delivering application-specific services to the user is the responsibility of the application layer. This outlines the different uses for IoT, such as smart cities and houses, among others.

On the other hand, as Figure 1.B illustrates, the 5-layer architecture consists of perception, transport, processing, application, and business layers. The perception and application layers in 5 layers are same as the architecture with 3 layers [1][2][3].

- Through networks like WiFi, 3G, LAN, Bluetooth, RFID, and NFC, the transport layer moves sensor data from the perception layer to the processing layer and vice versa.
- The middleware layer, also referred to as the processing layer, is responsible for managing and delivering a wide range of services to the lower layers while storing, analyzing, and processing massive volumes of data originating from the transport layer. Big data processing modules, cloud computing, databases, and other technologies are used by this layer.
- The business layer is responsible to manage the whole IoT system, including applications, business and profit models, and users' privacy.

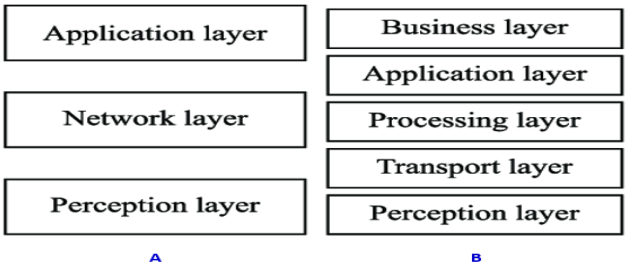

Figure 1. Internet of Things Architecture, 1.A: three layers & 1.B: five layers [3]

1.2. IoT Applications and Their usage

IoT application research is being conducted from more than a thousand angles. IoT applications offer several clever answers for the problems facing the world today, and they will also drastically alter it in the future. Numerous businesses worldwide have already made significant financial investments in the IoT space [3] [9]. This article presents a few prominent emerging IoT applications and their uses as follows while there are large number of other applications are available as shown in figure 2:

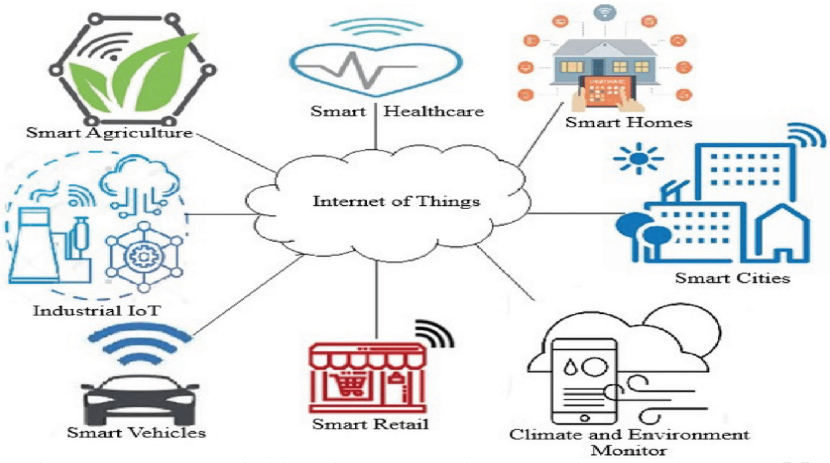

Figure 2: Internet of Things between end users and application areas [1]

1.2.1. Smart City

The most widely used application for solving everyday problems in urban areas is the smart city, which has numerous applications like as trash management, traffic and electricity management, water management, and so on. Seismic activity, wind pressure, and self-driving sensors in automated vehicles can all be detected by sensors attached to the building. These sensors also ensure that water and electricity supplies are used appropriately, and regular monitoring will improve the state of air and water pollution. Additionally, it will result in a rise in IT jobs [1][2][10].

1.2.2. Smart home

A system in which the internet is used to connect appliances, air conditioning, microwaves, refrigerators, washing machines, lights, doors, and security systems. Ultimately, smart gadgets increase security levels, save money and energy, protect household appliances from natural calamities, and even control internet-connected devices from anywhere in the world [3][6][10].

1.2.3. Connected Car

When an automobile can be operated by a smartphone or any other device that has a direct internet connection, it is said to be linked. Numerous sensors are used by the program to track the vehicle's present condition, anticipate mechanical failures before they happen, and take prompt action to prevent accidents. Moreover, voice command is accessible on smartphones and ultimately results in time savings [1][2][10].

1.2.4. Traffic Monitoring

Many underdeveloped or third-world countries still have antiquated traffic monitoring systems; traffic lights are typically manually watched, and insufficient surveillance keeps traffic violators out of reach. One of the clever solutions provided by IoT is the application of image processing. The surveillance cameras can identify and photograph anyone breaking the traffic laws, alerting the appropriate authorities to take appropriate action. This program can also count the number of vehicles on either side of the road and use the KNN algorithm to calculate the waiting times on each side. The amount of human labor needed to manage the traffic system will be greatly decreased. Additionally, research is being done to track stolen vehicles using Internet of Things applications [7][10][11].

1.2.5. Smart Grid

Electrical equipment, computer networks, automation, and power supplies make up the intelligent grid, which is a two-way communication system in between utility and consumer needs. It adjusts its reactions based on the needs of the user, for example, by detecting transmission lines to guarantee appropriate electrical supply, self-repairing (rerouting) power outages, and assisting users in lowering their electricity expenses by recommending low-priority electronic gadgets. It eventually offers the chance to boost a nation's productivity and efficiency by improving supply management [10][11][12].

2. Background

At the moment there are billions of devices linked to the internet. Therefore the Internet of Things is in charge of sending vast amounts of data every day. It can be imagined what happens when corporations don't put strong enough security measures into IoT devices, and that has started to become a real worry as more homes and businesses adopt such devices. It is evident from the past history that a lack of adequate security has contributed to an increase in security breaches globally. The following lists five IoT security breaches, along with an explanation of what happened and advice on how to avoid being a victim of a vulnerability.

I. **Stuxnet**: An extremely intelligent computer worm created to destroy Iran's nuclear enrichment plant at Natanz. When this worm is introduced into a network, it starts searching for centrifuges—devices that separate uranium isotopes—and re programs them to carry out different cycles that cause the centrifuges to malfunction. Due to the fact that the centrifuges are Internet of Things devices and are connected to a local network. It was one of the first times a computer worm has really destroyed hardware instead of just attacking it to cause software harm. The denial of service attack is an illustration of typical software damage. Stuxnet features numerous defenses, like self-disable and self-erasing, that keep it from being discovered on computers running specific security systems. Up to 1,000 centrifuges were destroyed by Stuxnet. The author of this particular worm has not been identified to far. This damage and security breach may have been prevented if the nuclear facilities' centrifuges had been operating on a rudimentary version of defensive software [31][32].

II. **Mirai botnet:** On October 21, 2016, Dyn, a business that offers domain name services to well-known corporations including Netflix, GitHub, Twitter, and Reddit, was attacked by the Mirai botnet. Mirai is a prime example of how designers of Internet of Things devices with publicly accessible software need to understand that the default login credentials need to be updated and may be exploited in malicious ways. Many IoT devices were compromised by the Mirai botnet in 2016.The majority of the compromised devices were older routers and IP cameras, which were then exploited to launch a DDoS attack against DNS service Dyn. Because most users don't update their device's default usernames and passwords, this malicious code took advantage of the old Linux kernel version. Etsy, GitHub, Netflix, Shopify, SoundCloud, Spotify, Twitter, and a number of other well-known websites were taken down by it [16]. This exploit serves as a wake-up call to many businesses who underinvest in their devices' storage capacity, preventing future Linux kernel updates. IoT devices will continue to be vulnerable to vulnerabilities as long as businesses are unwilling to invest enough in updating their systems [16]. It should go without saying that you should quickly change the default password and username on any Internet of Things device that is password secured. Another operation that resembled the Mirai botnet was Brickerbot, which also depended on a DDoS attack and consumers failing to modify their device's default login and password. Brickerbot merely destroys the device, which is the primary distinction between it and the Mirai botnet [31][32].

III. **The botnet barrage:** Verizon Wireless provided a report on the attack. This report disclosed that over 5,000 IoT devices were attacked, but it withheld the name of the university that was targeted. Senior IT staff members on campus identified this situation after receiving multiple complaints about the slow and unreliable network. They also discovered that an unusually high number of sub-domains linked to seafood was displayed by their name servers, along with a high volume of notifications [32]. Additionally, it was discovered that every fifteen minutes, more than 5,000 distinct systems were performing hundreds of DNS lookups. Using a brute force assault to crack weak passwords, a botnet expanded among all those IoT devices. Stronger passwords must be used to secure every IoT device, and constant monitoring of network activities is the only method to address this [32].

IV. **Casino Data Leak**: An online casino experienced a data leak involving over 108 million bets, as well as personal information, deposits, and other withdrawals [32]. Most people assume that hacking servers to obtain sensitive data entails breaking into the main server; however, in the casino's instance, the data was obtained through the aquarium. Older heaters used a basic thermostat, but more recent systems incorporate Internet of Things temperature sensors, which enable a central system to remotely monitor the aquarium. Most aquariums need a heater with a temperature monitor. However, the temperature sensor needs to be connected to a local network in order to access the internet. If Wi-Fi is used, it provides an avenue of access for outside attackers. The primary worry is that even the most basic internet-connected item has the ability to compromise even the most secure networks. An engineer only needs to choose not to add security to anything as basic as a temperature sensor [32][33].

V. **The Jeep Hack:** The number of automobiles connected to the Internet of Things is rising along with the car industry's expansion and significant advancements. More people are drawn to these cars because of its extra features, which include safety features and services for drivers. Safety and security are major concerns along with the motor industry's expansion and advancement. We occasionally learn of system hacking stories. The auto industry is extremely concerned about the Jeep breach since it could have disastrous effects on drivers' privacy and safety [34]. Furthermore, it will be extremely difficult to achieve widespread acceptance of smart cars if consumers have a strong fear of danger. This concern also extends to the fear of the smart car's discontinuation in the auto mobile business. Security researchers Chris Valasek and Charlie Miller gained access to a 2014 Jeep Cherokee through hacking in 2015, and they managed to spin the steering wheel, temporarily disengage the brakes, and turn off the engine [34]. Not content to stop there, these researchers also discovered that thousands of vehicles, including Dodge, Jeep, and Chrysler models, may be accessed and are at high risk by using the Uconnect wireless entertainment and navigation system [34]. It is not advisable to connect remotely accessible devices to a shared industry connection [31]. The ramifications are horrifying if the hackers are able to connect, access, and control safety components remotely while the cars are moving. Following this occurrence, automakers and transit providers are fortifying the security features in their vehicles. However, given that these new technologies are already making consumer travel safer, the advantages of smart automobiles in terms of convenience and safety greatly exceed their drawbacks [3].

3. Analysis of IoT Security Goals

The protection of gathered data is the main goal of IoT security. Any information gathered from a physical device may contain private user data. As a result, IoT systems must offer privacy, data security, and trust while being resistant to attacks involving data. IoT systems must use a variety of techniques, including data availability, redundancy, data encryption, access control, and authentication, backups, and more, to safeguard the confidentiality, integrity, and availability of the data. As long as the security objectives are upheld, trust is restored. Every IoT Layer needs to trust each other because to guarantee data security and privacy, there should be secure communication between every layer and every node. Ensuring the dependability, accuracy, and privacy of data at every IoT layer upholds confidence in its security and privacy. The end user and the IoT system must have trust in one another for the IoT idea to be implemented successfully, as the system will eventually reveal some information to the user and the user will provide some information to the system.

3.1. Security Attacks Classification of IoT

There are various ways through which an IoT system can be attacked. Attack can be mainly classified into four major groups as shown in the Table 1 below [13] while Security attacks on IoT more broadly can be classified into various categories based on the nature of the attacks and the vulnerabilities they exploit. Some common classifications of IoT security attacks are; Device-Level Attacks which targeting individual IoT devices to compromise their functionality, data, or integrity. For example, physical tampering, device spoofing, firmware attacks, and side-channel attacks. Network-Level Attacks means attacks that exploit vulnerabilities in the communication infrastructure and networks connecting IoT devices. For example, Man-in-the-middle attacks, eavesdropping, network spoofing, and denial-of-service (DoS) attacks [14], Application-Level Attacks are targeting the software applications and services that manage or utilize IoT data. Injection attacks (e.g., SQL injection), unauthorized access, insecure application interfaces, and malicious app downloads can be taken as the examples [15], Cloud-Based Attacks means exploit vulnerabilities in cloud-based IoT platforms and services where data is stored or processed. For instance, Data breaches, unauthorized access to cloud resources, and attacks on cloud-based APIs, Edge Computing Attacks target the edge computing devices and gateways that process and analyze IoT data locally. Here are some examples: Edge device compromise, tampering with locally stored data, and unauthorized access to edge computing resources [14][15][16].

Further we can classified such as, Protocol-Level attack that exploiting weaknesses in communication protocols used by IoT devices. For example, Protocol spoofing, replay attacks, and protocol vulnerabilities leading to unauthorized access, Physical Attacks involving physical access to IoT devices, aiming to manipulate or damage the hardware and the examples are Device theft, tampering, environmental attacks, and attacks involving physical destruction [17], Supply Chain Attacks are the attacks that target the supply chain of IoT devices, compromising their security during manufacturing, distribution, or installation. For example, Firmware manipulation during production, insertion of malicious components, and unauthorized modifications during shipping, Authentication and Authorization Attacks are focused on bypassing or exploiting weaknesses in authentication and authorization mechanisms [18]. Credential stuffing, brute-force attacks, and token manipulation are some examples of this attack, privacy violations are attacks that compromise the privacy of individuals or organizations by unauthorized access or disclosure of sensitive data collected by IoT devices. For example, unauthorized data access, data leaks, and location tracking without consent, IoT Botnet Attacks can be identified as the attacks that involve the compromise of multiple IoT devices to create a botnet for malicious activities [19]. The examples are, Mirai botnet, which targeted IoT devices for large-scale distributed denial-of-service (DDoS) attacks, Data Manipulation Attacks known as the attacks that involve altering or manipulating the data collected, transmitted, or processed by IoT devices. For example, Data tampering, injection attacks, and manipulation of sensor readings, Zero-Day Exploits means the attacks that target vulnerabilities in IoT devices or software that are not yet known to the vendor or the public. Here are some examples, exploiting newly discovered vulnerabilities before patches or fixes are available, Social Engineering Attacks manipulate individuals or users to divulge sensitive information or take malicious actions. For example, Phishing attacks, baiting, and impersonation to gain unauthorized access [17][18][19][20].

Understanding the different categories of IoT security attacks is crucial for developing comprehensive security strategies. Organizations must implement a combination of preventive measures, detection mechanisms, and response strategies to mitigate the risks associated with these diverse attack vectors. Regular security assessments and updates are essential to adapt to evolving threats in the dynamic IoT landscape.

<table>
<tr><th>Physical Attacks</th><th>Network Attacks</th><th>Software Attacks</th><th>Encryption Attacks</th></tr>
<tr><td>Node Tampering</td><td>Traffic Analysis Attacks</td><td rowspan="2">Virus and Worms</td><td>Side Chanel Attacks</td></tr>
<tr><td>RF Interference</td><td>RFID Spoofing</td><td rowspan="5">Cryptanalysis Attacks:
a) Ciphertext Only Attack
b) Known Plaintext Attack
c) Chosen Plaintext or Ciphertext Attack</td></tr>
<tr><td>Node Jamming</td><td>RFID Cloning</td><td rowspan="2">Spyware and Adware</td></tr>
<tr><td>Malicious Node Injection</td><td>RFID Unauthorised Access</td></tr>
<tr><td>Physical Damage</td><td>Sinkhole Attack</td><td rowspan="2">Trojan Horse</td></tr>
<tr><td>Social Engineering</td><td>Man In the Middle Attack</td></tr>
<tr><td rowspan="2">Sleep Deprivation Attack</td><td rowspan="2">Denial of Service</td><td rowspan="2">Malicious scripts</td><td rowspan="3">Man In the Middle Attack</td></tr>
<tr><td rowspan="2">Routing Information Attacks</td></tr>
<tr><td rowspan="2">Malicious Code Injection on the Node</td><td rowspan="2">Denial of Service</td></tr>
<tr><td>Sybil Attack</td></tr>
</table>

Table 1: Summary of IoT Attacks Classification [13]

3.2. IoT Firmware & Application Vulnerability Detection: Methods and Challenges

Vulnerability detection in IoT firmware and application are essential for ensuring the security of IoT devices. Firmware vulnerabilities can expose devices to various threats, including unauthorized access, data breaches, and potential exploitation for malicious purposes [21][24]. Some approaches and best practices for detecting vulnerabilities in IoT firmware are; Static Code Analysis which use automated tools for static code analysis to review the source code for vulnerabilities. These tools can identify common coding errors, security flaws, and potential weaknesses in the firmware. Check for insecure coding practices such as buffer overflows, format string vulnerabilities, and improper input validation [22], Dynamic Analysis employ dynamic analysis techniques by executing the firmware in a controlled environment and monitoring its behavior. This can help identify runtime vulnerabilities and potential security issues, use fuzz testing to inject malformed or unexpected inputs into the firmware to discover vulnerabilities related to input validation and handling [23], Penetration Testing conduct penetration testing to simulate real-world attacks on the IoT device. This involves actively probing the device for weaknesses, attempting to exploit vulnerabilities, and assessing the overall security posture. Focus on areas such as authentication mechanisms, communication protocols, and data storage to identify potential vulnerabilities, Code Reviews conduct thorough code reviews with a focus on security [21][23]. Involve experienced security professionals who can identify vulnerabilities and suggest improvements. Review third-party libraries and components for known vulnerabilities and ensure that they are up to date, Secure Coding Standards adhere to secure coding standards and best practices. Follow guidelines such as CERT Secure Coding Standards, OWASP IoT Top 10, and other industry-specific standards. Ensure that developers are trained in secure coding practices and are aware of potential security pitfalls, Dependency Scanning regularly scan firmware dependencies for known vulnerabilities. Many IoT devices use third-party libraries and components, and vulnerabilities in these dependencies can pose a significant risk. Keep dependencies updated and apply patches promptly when security vulnerabilities are discovered, Network Security Implement secure communication protocols, such as TLS/SSL, to protect data in transit [22][23]. Use strong encryption and authentication mechanisms. Perform network vulnerability assessments to identify weaknesses in the device's network interfaces, Device Configuration and Hardening ensure that default credentials are changed, unnecessary services are disabled, and the device is configured securely. Implement secure boot mechanisms to prevent unauthorized firmware modifications, Monitoring and Logging implement robust logging mechanisms to capture and analyze security-related events. This can aid in detecting and responding to potential security incidents. Set up intrusion detection systems to monitor for suspicious activities, Security Updates and Patch Management establish a process for delivering and applying security updates to the firmware. Regularly check for updates from the device manufacturer and apply patches promptly provide mechanisms for users to easily update firmware, promoting a culture of patching and security hygiene [21][22][23].

Regular and systematic security assessments, combined with a proactive approach to addressing vulnerabilities, are essential for maintaining the security of IoT firmware and applications. It's crucial to stay informed about the latest security threats and continuously improve the security posture of IoT devices throughout their lifecycle. In addition, addressing the specific challenges associated with the IoT ecosystem requires specialized tools, expertise, and a holistic understanding of the interconnected systems involved. Regular updates and collaboration within the security community are essential for staying ahead of emerging threats in the evolving landscape of IoT security.

Table 2 indicates that logical weaknesses such as XSS, injection, and authentication-bypass primarily affect web servers like Apache and web applications like WordPress and phpMyAdmin cannot result in system crashes, whereas binary applications and operating systems like Excel, Linux, and Android are more prone to have memory flaws like buffer-overflows, which frequently cause system crashes [24]. A significant portion of IoT devices, such as routers and cameras, include firmware that contains memory vulnerabilities and a few logical problems. This is partly because, unlike most websites, which utilize scripts like PHP, ASP, and JSP, most Internet of Things devices have web interfaces that are vulnerable to logical errors and are typically implemented using binary CGIs [24].

Targets	XSS	Inject	Authentication -bypass	Overflow
Wordpress	51.4%	39.2%	1.3%	0%
phpMyAdmin	38.5%	36.9%	1.2%	0%
Apache	12.9%	9.6%	4.8%	4.8%
Router	7.9%	6.7%	6.5%	6.5%
Camera	9.3%	12.6%	3.7%	10.2%
Firmware	9.8%	10.6%	5.5%	7.2%
Excel	1.4%	0.7%	0%	19.4%
Linux	1.2%	1.3%	0.7%	15.6%
Android	0.6%	0.7%	0.1%	6.8%

Table 2: Ratios of different vulnerabilities in different targets [24]

As shown in the figure 5, identifying vulnerabilities in IoT firmware, especially when dealing with binaries and the MIPS architecture, presents unique challenges that distinguish it from vulnerability detection in traditional software. Some key points related to this specific context are Limited Access to Source Code In many cases, IoT firmware developers may not provide access to the source code, making it challenging to perform source code-based vulnerability analysis. This limitation is common in proprietary firmware or when dealing with closed-source components, CGIs and Binary-Only Representation CGI (Common Gateway Interface) scripts in IoT firmware, responsible for executing specific operations, may be available only as binaries. This poses a challenge for traditional logical flaw audit techniques that typically require access to source code for a comprehensive analysis, Fuzzing Challenges fuzzing tools like AFL (American Fuzzy Lop) are effective for identifying memory vulnerabilities through the observation of crashes. However, they may not be as effective in identifying logical flaws or issues related to the business logic of the application [25][26]. Fuzzing binary-only representations might reveal memory-related vulnerabilities but could miss deeper logical issues, Symbolic Execution Limitations symbolic execution tools, like S2E, can analyze binaries at the symbolic level to identify vulnerabilities. However, their effectiveness may be limited when it comes to logical flaws or complex business logic issues that require a deeper understanding of the application's behavior, MIPS Architecture Challenges the prevalence of the MIPS architecture in embedded systems, as opposed to the more common x86 architecture, poses challenges for existing tools that are often designed for x86. MIPS-based binaries may require specialized analysis tools that understand the intricacies of this architecture, Limited Tool Support for MIPS indeed, there are fewer tools available that explicitly support the MIPS architecture compared to x86. This scarcity of tools may hinder the vulnerability detection process for IoT firmware based on MIPS [25] [26] [27].

To address these challenges, security researchers and practitioners working on IoT firmware vulnerability detection in binary form need to consider the things such as specialized Tools for MIPS Look for or develop tools that specifically support the MIPS architecture. This may involve adapting existing tools or creating new ones tailored to the unique aspects of the MIPS instruction set, Emulation and Simulation use emulation or simulation environments that support the MIPS architecture. This can provide a controlled environment for analyzing binary code without the need for physical devices [27][28], Collaboration and Knowledge Sharing given the specialized nature of IoT firmware analysis, collaboration within the security research community is essential. Sharing knowledge, tools, and techniques can help overcome challenges collectively, Reverse Engineering Expertise developing expertise in reverse engineering, especially in the context of MIPS binaries, is crucial. Skilled reverse engineers can manually analyze binary code to identify logical flaws, business logic issues, and potential vulnerabilities, Firmware Extraction and Analysis explore techniques for extracting firmware from IoT devices. Once extracted, the firmware can be analyzed in a controlled environment where researchers have more flexibility in applying various analysis techniques [29][30]. In conclusion, the identification of vulnerabilities in IoT firmware, particularly when dealing with binary representations and the MIPS architecture, requires a combination of specialized tools, expertise in reverse engineering, and collaborative efforts within the security community to address the unique challenges posed by these environments.

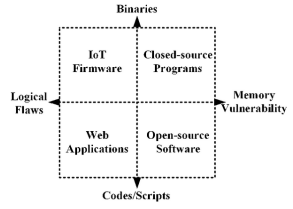

Figure 3. Comparisons of vulnerability detection in different targets [24]

3.3. IoT Network Vulnerability Detection: Methods and Challenges

Detecting vulnerabilities in IoT networks is essential for maintaining the security of interconnected devices. Various methods and techniques can be employed, but they come with their own set of challenges. Some of the methods and challenges associated with IoT network vulnerability detection are Network Scanning which use tools like Nmap, Nessus, or OpenVAS to scan the IoT network for open ports, services, and potential vulnerabilities. Challenges can be disruptions to resource-constrained IoT devices, and false positives/negatives are possible, Penetration Testing can be used as employ ethical hacking techniques to simulate real-world attacks on the IoT network, identify vulnerabilities, and assess overall security and the challenges are resource-intensive, may disrupt network operations, and requires careful planning to avoid unintentional damage, Protocol Analysis can be used to analyze the communication protocols used in the IoT network for potential vulnerabilities, ensuring proper encryption (e.g., TLS/SSL) [35]. The challenges are understanding and interpreting proprietary or custom protocols can be complex, and detecting subtle protocol-level vulnerabilities may be challenging, Device Authentication and Access Controls can be used to evaluate the authentication mechanisms and access controls on IoT devices to prevent unauthorized access. Challenges are, Weak or default credentials, lack of uniform authentication standards across devices, and the need for secure credential management, Security Configuration Review the security configurations of network devices, gateways, and routers to identify and mitigate vulnerabilities. The challenges are overlooking specific device configurations, potential misconfigurations, and ensuring consistency across all network components, Wireless Network Security assess the security of wireless communication, including Wi-Fi or other wireless protocols, to prevent unauthorized access. Challenges of this method are, securing diverse wireless communication protocols, avoiding interference, and protecting against advanced wireless attacks, IoT Gateway Security evaluate the security of IoT gateways, ensuring secure communication between devices and gateways, and implementing security measures. Challenges can be listed as, Gateway-specific vulnerabilities, managing data aggregation securely, and protecting gateways from compromise, Network Segmentation implement network segmentation to isolate IoT devices from critical infrastructure and other sensitive systems. The challenges are, defining proper segmentation policies, avoiding unintended consequences of segmentation, and ensuring effective communication between segments, Intrusion Detection and Prevention Systems (IDPS) deploy IDPS to monitor network traffic for suspicious activities and take preventive actions in response to detected anomalies and the challenges could be, tuning IDPS for low false positives, keeping signatures up to date, and detecting sophisticated, low-and-slow attacks, Data Encryption implement end-to-end encryption for data transmitted between IoT devices and backend systems or cloud services [35][36]. The challenges are managing cryptographic keys securely, avoiding performance degradation, and ensuring compatibility with diverse IoT devices, Continuous Monitoring implement continuous monitoring of the IoT network to detect and respond to security incidents in real-time. The challenges are handling large volumes of data generated by monitoring solutions, distinguishing normal traffic from malicious behavior, and responding promptly to incidents, Firmware and Software Updates regularly update and patch firmware and software on IoT devices and network infrastructure and the challenges are authenticating firmware updates, ensuring compatibility with diverse devices, and providing mechanisms for users to easily update IoT devices [35][36][37]. In summary, vulnerability detection in IoT networks requires a careful balance between assessing device-specific vulnerabilities, securing communication protocols, and ensuring the overall resilience of the interconnected ecosystem. The challenges associated with the diverse nature of IoT deployments and the need for cross-industry collaboration highlight the complexity of securing these networks effectively.

4. Results: Defensive Techniques and Methods to Mitigate Data Breaches

As we discussed earlier in this article, figure 1A, there are three main distinct layers in an Internet of Things at the high-level architecture, each with potential security flaws. Therefore, a multi-layered security method might be considered to successfully defend the IoT system and avoid these assaults [13] as listed below for each layer and summery of all the defensive measures are listed in the Table 3.

4.1. Perception Layer Security for IoT

Securing the Perception Layer in IoT (Internet of Things) is crucial because it involves the collection of data from the physical world through sensors and devices. Ensuring the integrity, confidentiality, and availability of this data is essential. Some key strategies for implementing Perception Layer Security in IoT are, Device Authentication and Authorization which implement strong authentication mechanisms for IoT devices at the Perception Layer. Devices should be uniquely identified and authenticated before they are granted access to the network or start transmitting data, Secure Device Bootstrapping that ensures secure bootstrapping processes for devices to establish a secure initial connection with the network. This involves securely provisioning devices with the necessary credentials and configurations, Secure Communication Protocols which uses secure and encrypted communication protocols for data transmission between IoT devices and gateways or edge devices. Employ protocols such as CoAP (Constrained Application Protocol) or MQTT (Message Queuing Telemetry Transport)

with appropriate security measures [38], Data Integrity and Authenticity to implement mechanisms to ensure the integrity and authenticity of the data collected by sensors. This may involve using digital signatures, checksums, or cryptographic hashes to verify that the data has not been tampered with during transmission, Secure Wireless Communication means if wireless communication is involved, secure wireless protocols and standards should be used. Employ encryption (e.g., WPA3 for Wi-Fi) to protect data in transit and implement secure key exchange mechanisms, Secure Physical Connections for wired connections, ensure physical security of the connections to prevent tampering. Use tamper-evident seals or enclosures to detect and respond to physical attacks on the devices or sensors, Secure Device Configuration implement secure configurations for IoT devices. Default credentials should be changed, unnecessary services should be disabled, and security features (e.g., firewalls) should be enabled to reduce the attack surface, Physical Unclonable Functions (PUFs) Utilize PUFs to uniquely identify and authenticate IoT devices based on their physical characteristics [39]. PUFs enhance device security by making it difficult for attackers to clone or replicate device identities, Device Firmware Integrity ensure the integrity of device firmware.

Additionally, Implement secure boot processes and firmware updates to prevent unauthorized modifications. Devices should only accept updates from trusted and authenticated sources, Environmental Considerations account for environmental factors when securing devices in the Perception Layer. For example, devices deployed outdoors may be vulnerable to physical damage, and protections should be in place to mitigate these risks [39], Security Monitoring implement continuous monitoring of the Perception Layer. This includes monitoring for abnormal sensor readings, unexpected device behaviors, or any signs of unauthorized access or tampering, Privacy by Design Integrate privacy considerations into the design of IoT devices and systems. Minimize the collection of personally identifiable information (PII) and ensure compliance with privacy regulations, Secure Device Lifecycle Management establish secure processes for device provisioning, operation, and decommissioning. This includes secure onboarding, periodic security checks, and secure disposal or repurposing of devices at the end of their lifecycle, Physical Security Measures Implement physical security measures to protect sensors and devices from physical attacks. This may include secure enclosures, tamper-resistant designs, and secure mounting of devices, Integration with Network Security ensure that security measures at the Perception Layer are seamlessly integrated with broader network security strategies. This involves coordination with network segmentation, firewalls, and intrusion detection systems [40]. By implementing these strategies, organizations can enhance the security of the Perception Layer in IoT, protecting the data collected by sensors and ensuring the reliability and trustworthiness of the information flowing into the IoT ecosystem. Regular security assessments, monitoring, and updates are crucial to adapt to evolving threats and vulnerabilities.

4.2. Network Layer Security for IoT

The network layer, which is primarily in charge of ensuring that every item in the Internet of Things system is connected via variety of communication protocols, comprises network administration, network interfaces, communication channels, intelligent processing, and information maintenance. MQTT and CoAP are the two most often utilized protocols [13]. Securing the Network Layer is a crucial aspect of IoT security, as it involves the communication between devices and the transfer of data across networks. Some key strategies for implementing Network Layer Security in IoT are, Secure Communication Protocols Which Use secure and encrypted communication protocols for data transmission between IoT devices, gateways, and backend systems. Protocols such as MQTT (Message Queuing Telemetry Transport) with TLS (Transport Layer Security) provide a secure communication framework, Virtual Private Networks (VPNs) implement VPNs to create secure, private communication channels over public networks. VPNs encrypt data traffic, providing an additional layer of security for IoT devices communicating over the internet [38][41], Network Segmentation Segment IoT devices into separate networks based on their functions and security requirements. This helps contain potential security breaches and limits lateral movement within the network, Intrusion Detection and Prevention Systems (IDPS) Deploy IDPS to monitor network traffic for suspicious activities and potential security threats. IDPS can detect and respond to anomalies, helping to prevent unauthorized access or attacks, Firewalls Implement firewalls to control and monitor traffic between different network segments [39]. Firewalls can enforce security policies, filter traffic, and block unauthorized access attempts, Quality of Service (QoS) Enforcement use QoS mechanisms to prioritize and manage network traffic. This ensures that critical IoT data receives preferential treatment, improving overall network performance and reliability, Security Gateways deploy security gateways to act as intermediaries between IoT devices and backend systems [42]. Security gateways can enforce security policies, perform authentication, and encrypt data before it reaches the backend, Traffic Encryption encrypt data in transit using protocols like IPsec (Internet Protocol Security) or TLS. This protects sensitive information from eavesdropping and tampering during transmission, Device Authentication and Authorization implement strong authentication mechanisms for devices connecting to the network. Use methods like mutual TLS authentication to ensure that both the device and the server authenticate each other, Network Monitoring and Logging monitor network traffic and maintain detailed logs for analysis. Analyzing logs can help identify unusual patterns, detect

security incidents, and facilitate timely responses to potential threats, Denial of Service (DoS) Mitigation implement measures to mitigate DoS attacks, which can disrupt IoT services. This may involve rate limiting, traffic filtering, and the use of content delivery networks (CDNs) to distribute and handle traffic, IPv6 Security Considerations if using IPv6 in IoT networks, be aware of and address specific security considerations associated with this protocol. Ensure that security controls are adapted to the IPv6 environment [43], Secure Firmware Updates ensure that firmware updates for IoT devices are securely delivered and applied. This prevents the exploitation of known vulnerabilities and ensures the ongoing security of the devices; Secure Time Synchronization use secure time synchronization mechanisms to ensure that devices in the IoT network have accurate and synchronized time. This is crucial for security protocols and helps prevent attacks that rely on time-related vulnerabilities [24][43], Zero Trust Network Model Adopt a Zero Trust model, where every device and user is treated as untrusted until proven otherwise. This approach involves continuous verification and monitoring of devices, even those within the internal network [41][42][43]. Implementing these Network Layer security measures helps create a robust and secure foundation for IoT deployments, reducing the risk of unauthorized access, data breaches, and other security threats. Regular security assessments and updates are essential to adapt to evolving threats in the dynamic IoT landscape.

4.3. Application Layer Security for IoT

Securing the Application Layer in the context of IoT is vital to protect sensitive data and ensure the proper functioning of IoT applications. Some of the key strategies for implementing Application Layer Security in IoT are API Security which ensure secure communication between IoT devices, applications, and backend systems using well-designed APIs. Implement strong authentication, authorization, and encryption for API endpoints [44]. Validate input data to prevent injection attacks, Secure Communication Protocols which use secure and well-established communication protocols for transmitting data between IoT devices and applications. Implement encryption (e.g., TLS/SSL) to protect data in transit, preventing eavesdropping and tampering, Authentication and Authorization implement robust authentication mechanisms for users, devices, and applications [35][43]. Use strong, unique credentials, and consider multi-factor authentication to enhance security. Authorize access based on the principle of least privilege, Tokenization and Session Management implement tokenization for managing user sessions and device interactions. Use short-lived tokens with proper expiration periods, and secure session management practices to prevent session hijacking, Data Validation and Sanitization validate and sanitize all inputs to prevent common vulnerabilities such as SQL injection, cross-site scripting (XSS), and other injection attacks. Implement input validation at both the client and server sides, Secure Coding Practices train developers in secure coding practices. Conduct regular code reviews and static code analysis to identify and remediate security vulnerabilities in IoT application code, Security Headers use security headers in web applications to provide an additional layer of protection. Headers like Content Security Policy (CSP) and Strict-Transport-Security (HSTS) help mitigate various web-based attacks, Security Patching and Updates keep all software components, libraries, and frameworks up to date with the latest security patches. Regularly update and patch applications to address known vulnerabilities and security issues, Secure File Uploads is important if your IoT application involves file uploads, implement secure practices to validate and handle uploaded files [45]. Ensure that file types are properly checked, and implement size limits to prevent abuse, Secure Third-Party Integrations are if your IoT application relies on third-party integrations, thoroughly vet and secure those integrations. Ensure that third-party APIs are secure and adhere to the same security standards as your application, Data Encryption and Decryption encrypt sensitive data at rest within the application database. Implement proper key management practices to secure encryption keys, and consider using hardware security modules (HSMs) for additional protection [46], Logging and Monitoring implement comprehensive logging to record security-relevant events within the application. Set up continuous monitoring and alerting to quickly identify and respond to any suspicious activities, User Education and Awareness educate end-users about security best practices, such as creating strong passwords, recognizing phishing attempts, and understanding the security features of the IoT application [47]. Enhance user awareness to prevent social engineering attacks, Incident Response Plan develop and regularly test an incident response plan specific to IoT application security. Define procedures for identifying, containing, eradicating, recovering from, and analyzing security incidents, Secure Device Provisioning and Decommissioning establish secure processes for onboarding and decommissioning IoT devices. Ensure that devices are properly authenticated during the provisioning phase, and remove access and data associated with decommissioned devices securely, Container Security (if applicable) is important if the IoT application is containerized, ensure container security by scanning images for vulnerabilities, restricting container privileges, and adopting best practices for securing containerized environments [48]. By implementing these Application Layer security measures, organizations can enhance the overall security of their IoT applications and mitigate potential risks. Regular security assessments, penetration testing, and continuous monitoring are essential for identifying and addressing emerging threats in the rapidly evolving IoT landscape.

IoT Layer	Counter Attacks for the Specific Layers	Counter Attacks for All Layers
Physical Layer	1) Secure Booting for all IoT devices a) Low power Cryptographic Hash Functions 2) Device Authentication using Low Power Techniques a) Data Integrity b) CRC – Cyclic Reduntancy Check c) Checsum d) Parity Bit e) WH Cryptographic Hash Function 3) Data Confidentiality a) Encryption Algorithms like Blowfish and RSA 4) Data Anonimity a) K- Anonimity	1) Risk Assessment b) Finding New Threats c) Applying Updates d) Applying Patches e) Providing Improvements f) Upgrading Systems 2) Intrusion Detection Mechanisms specific to IoT Systems 3) Securing the IoT Premises a) Physical Barriers b) Intrusion Detection Alarms c) Monitoring Devices d) Access Control Devices e) Security Personel 4) Trust Management a) Trust relation between layers b) Trust of Security and Privacy at each layer c) Trust betweeen IoT and User
Network Layer	1) Secure Communication between the devices a) Network Authentication – challenge-response mechanisms b) Point-to-Point Encryption for the confidentiality of the transmited Data c) Cryptographic Hash Functions for the Inegrity of the transmited Data 2) Implementation of Routing Security a) Use of Multiple Paths b) Encrypting Routing Tables c) Hashing Routing Tables 3) Secure User Data on the Devices a) Data Authentication b) Data Confidentiality; Encryption Schemes of encrypting the data c) Data Integrity; Cryptographic hash functions	
Application Layer	1) Data Security a) Authentication; biometrics, passwords, etc. b) Confidentiality; Strong Encryption Schemes (AES) c) Integrity; Cyrptographic Hash Functions 2) Access Control Lists (ACLs) 3) Firewalls 4) Protective Software a) Anti-virus b) Anti-adware	

Table 3: Defensive Security Measures [13]

5. Conclusion

As the summery of this research, it can be concluded that, the Internet of Things is advancing into every industry in an attempt to revolutionize both the productivity of businesses and the quality of life for individuals. The Internet of Things (IoT) offers enormous potential to enable extensions and enhancements to basic services in many areas, including transportation, logistics, utilities, education, healthcare, and other areas, while offering a new ecosystem for application development. This is achieved through a widely dispersed, locally intelligent network of smart devices. Driven by a shared understanding of the unique nature of the opportunity, a deliberate effort is needed to propel the industry past the early stages of market development towards maturity. In addition to the benefits of IoT discussed in this study, it is evident that there are some drawbacks, such as the potential for data breaches and other attacks, including software, network, physical, and encryption attacks. Hence, the confidentiality, availability, and integrity of data are directly threatened by these attacks. Therefore, IoT systems are mostly susceptible to these attacks because of their low power and processing capabilities. Nonetheless, the vulnerability level can be somewhat reduced by utilizing layered security solutions that accommodate low processors.

References

[1] Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future generation computer systems 29, no. 7 (2013): 1645-1660.
[2] Khan, Saad, and Akalanka B. Mailewa. "Discover Botnets in IoT Sensor Networks: A Lightweight Deep Learning Framework with Hybrid Self-Organizing Maps." Microprocessors and Microsystems (2023): 104753.
[3] Sethi, Pallavi, and Smruti R. Sarangi. "Internet of things: architectures, protocols, and applications." Journal of electrical and computer engineering 2017 (2017).
[4] Jairu, Pankaj, and Akalanka B. Mailewa. "Network Anomaly Uncovering on CICIDS-2017 Dataset: A Supervised Artificial Intelligence Approach." In 2022 IEEE International Conference on Electro Information Technology (eIT), pp. 606-615. IEEE, May 2022.
[5] Mazi, Hilary, Foka Ngniteyo Arsene, and Akalanka Mailewa Dissanayaka. "The influence of black market activities through dark web on the economy: a survey." In The Midwest Instruction and Computing Symposium. (MICS), Milwaukee School of Engineering and Northwestern Mutual, Milwaukee, Wisconsin. 2020.
[6] Malche, Timothy, and Priti Maheshwary. "Internet of Things (IoT) for building smart home system." In 2017 International conference on I-SMAC (IoT in social, mobile, analytics and cloud)(I-SMAC), pp. 65-70. IEEE, 2017.
[7] Sharma, Vandana, and Ravi Tiwari. "A review paper on "IOT" & It's Smart Applications." International Journal of Science, Engineering and Technology Research (IJSETR) 5, no. 2 (2016): 472-476.
[8] Howell, J. (n.d.). Retrieved from https://technology.ihs.com/596542/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030-ihs-markit-says
[9] Khan, Muhammad Maaz Ali, Enow Nkongho Ehabe, and Akalanka B. Mailewa. "Discovering the Need for Information Assurance to Assure the End Users: Methodologies and Best Practices." In 2022 IEEE International Conference on Electro Information Technology (eIT), pp. 131-138. IEEE, May 2022.
[10] Rakib Chowdhury. (2019, September 14). Top 20 Most Remarkable IoT Applications in Today's World. Retrieved September 23, 2019, from UbuntuPIT website: https://www.ubuntupit.com/most-remarkable-iot-applications-in-todays-world/

[11] Khan, Shehram Sikander, and Akalanka Bandara Mailewa. "Detecting Network Transmission Anomalies using Autoencoders-SVM Neural Network on Multi-class NSL-KDD Dataset." In 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)
[12] Mailewa Dissanayaka, Akalanka, Roshan Ramprasad Shetty, Samip Kothari, Susan Mengel, Lisa Gittner, and Ravi Vadapalli. "A review of MongoDB and singularity container security in regards to hipaa regulations." In Companion Proceedings of the10th International Conference on Utility and Cloud Computing, pp. 91-97. 2017
[13] Andrea, Ioannis, Chrysostomos Chrysostomou, and George Hadjichristofi. "Internet of Things: Security vulnerabilities and challenges." In 2015 IEEE symposium on computers and communication (ISCC), pp. 180-187. IEEE, 2015.
[14] Mailewa, Akalanka, Susan Mengel, Lisa Gittner, and Hafiz Khan. "Mechanisms and techniques to enhance the security of big data analytic framework with mongodb and Linux containers." Array 15 (2022): 100236.
[15] Sridhar, Siddharth, Adam Hahn, and Manimaran Govindarasu. "Cyber–physical system security for the electric power grid." Proceedings of the IEEE 100, no. 1 (2011): 210-224.
[16] Rozendaal, Kyle, and Akalanka Mailewa. "Neural Network Assisted IDS/IPS: An Overview of Implementations, Benefits, and Drawbacks." International Journal of Computer Applications 975: 8887. [17]
[17] Kaja, Durga Venkata Sowmya, Yasmin Fatima, and Akalanka B. Mailewa. "Data integrity attacks in cloud computing: A review of identifying and protecting techniques." Journal homepage: www. ijrpr. com ISSN 2582 (2022): 7421.
[18] Tournier, Jonathan, François Lesueur, Frédéric Le Mouël, Laurent Guyon, and Hicham Ben-Hassine. "A survey of IoT protocols and their security issues through the lens of a generic IoT stack." Internet of Things 16 (2021): 100264.
[19] Damghani, Hamidreza, Leila Damghani, Heliasadat Hosseinian, and Reza Sharifi. "Classification of attacks on IoT." In 4th international conference on combinatorics, cryptography, computer science and computation. 2019.
[20] Dissanayaka, Akalanka Mailewa, Susan Mengel, Lisa Gittner, and Hafiz Khan. "Dynamic & portable vulnerability assessment testbed with Linux containers to ensure the security of MongoDB in Singularity LXCs." In Companion Conference of the Supercomputing-2018 (SC18). 2018.
[21] Yaqoob, Tahreem, Haider Abbas, and Mohammed Atiquzzaman. "Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review." IEEE Communications Surveys & Tutorials 21, no. 4 (2019): 3723-3768.
[22] Mailewa, Akalanka, and Jayantha Herath. "Operating Systems Learning Environment with VMware" In The Midwest Instruction and Computing Symposium.
[23] Shetty, Roshan Ramprasad, Akalanka Mailewa Dissanayaka, Susan Mengel, Lisa Gittner, Ravi Vadapalli, and Hafiz Khan. "Secure NoSQL based medical data processing and retrieval: the exposome project." In Companion Proceedings of the10th International Conference on Utility and Cloud Computing, pp. 99-105. 2017.
[24] Xie, Wei, Yikun Jiang, Yong Tang, Ning Ding, and Yuanming Gao. "Vulnerability detection in iot firmware: A survey." In 2017 IEEE 23rd International conference on parallel and distributed systems (ICPADS), pp. 769-772. IEEE, 2017.
[25] Eceiza, Maialen, Jose Luis Flores, and Mikel Iturbe. "Fuzzing the internet of things: A review on the techniques and challenges for efficient vulnerability discovery in embedded systems." IEEE Internet of Things Journal 8, no. 13 (2021): 10390-10411.
[26] Dissanayaka, Akalanka Mailewa, Susan Mengel, Lisa Gittner, and Hafiz Khan. "Vulnerability prioritization, root cause analysis, and mitigation of secure data analytic framework implemented with mongodb on singularity linux containers." In Proceedings of the 2020 the 4th International Conference on Compute and Data Analysis, pp. 58-66. 2020.
[27] Phu, Tran Nghi, Kien Hoang Dang, Dung Ngo Quoc, Nguyen Tho Dai, and Nguyen Ngoc Binh. "A novel framework to classify malware in MIPS architecture-based IoT devices." Security and Communication Networks 2019 (2019): 1-13.
[28] Ndri, Anna, Divya Bellamkonda, and Akalanka B. Mailewa. "Applications of Block-Chain Technologies to Enhance the Security of Intrusion Detection/Prevention Systems: A Review." In Midwest Instruction and Computing Symposium (MICS), vol. 2, p. 4. 2022.
[29] Quadir, Shahed E., Junlin Chen, Domenic Forte, Navid Asadizanjani, Sina Shahbazmohamadi, Lei Wang, John Chandy, and Mark Tehranipoor. "A survey on chip to system reverse engineering." ACM journal on emerging technologies in computing systems (JETC) 13, no. 1 (2016): 1-34.
[30] Mailewa, Akalanka, and Kyle Rozendaal. "A Novel Method for Moving Laterally and Discovering Malicious Lateral Movements in Windows Operating Systems: A Case Study." Advances in Technology (2022): 291-321, ISSN 2773-7098.
[31] Maker.IO (2019, February 20) "5 Leading IoT Security Breaches and What We Can Learn From Them." .Retrieved from https://www.digikey.com/En/Maker/Blogs/2019/5-Leading-Iot-Security-Breaches-and-What-We-Can-Learn-from-Them
[32] Wallen, J. (2017, June 13). Five nightmarish attacks that show the risks of IoT security. Retrieved from ZDNet website: https://www.zdnet.com/article/5-nightmarish-attacks-that-show-the-risks-of-iot-security/
[33] Catalin Cimpanu. (2019, January 22). Online casino group leaks information on 108 million bets, including user details. Retrieved from ZDNet website: https://www.zdnet.com/article/online-casino-group-leaks-information-on-108-million-bets-including-user-details/
[34] Wenzel, Scott L. "Not even remotely liable: Smart car hacking liability." U. Ill. JL Tech. & Pol'y (2017): 49.
[35] Dissanayaka, Akalanka Mailewa, Susan Mengel, Lisa Gittner, and Hafiz Khan. "Security assurance of MongoDB in singularity LXCs: an elastic and convenient testbed using Linux containers to explore vulnerabilities." Cluster Computing 23 (2020): 1955-1971.
[36] Perwej, Yusuf, Nikhat Akhtar, Neha Kulshrestha, and Pavan Mishra. "A Methodical Analysis of Medical Internet of Things (MIoT) Security and Privacy in Current and Future Trends." Journal of Emerging Technologies and Innovative Research 9, no. 1 (2022): d346-d371.
[37] Simkhada, Emerald, Elisha Shrestha, Sujan Pandit, Upasana Sherchand, and Akalanka Mailewa Dissanayaka. "Security threats/attacks via botnets and botnet detection & prevention techniques in computer networks: a review." In The Midwest Instruction and Computing Symposium.(MICS), North Dakota State University, Fargo, ND. 2019.
[38] Seoane, Victor, Carlos Garcia-Rubio, Florina Almenares, and Celeste Campo. "Performance evaluation of CoAP and MQTT with security support for IoT environments." Computer Networks 197 (2021): 108338.
[39] Shamsoshoara, Alireza, Ashwija Korenda, Fatemeh Afghah, and Sherali Zeadally. "A survey on physical unclonable function (PUF)-based security solutions for Internet of Things." Computer Networks 183 (2020): 107593.
[40] Sapkota, Bhumika, and Akalanka B. Mailewa. "A Scalable Framework to Detect, Analyze, and Prevent Security Vulnerabilities in Enterprise Software-Defined Networks." Journal homepage: www. ijrpr. com ISSN 2582: 7421.
[41] Mathews, Suja P., and Raju R. Gondkar. "Protocol recommendation for message encryption in MQTT." In 2019 International Conference on Data Science and Communication (IconDSC), pp. 1-5. IEEE, 2019.
[42] Kimbugwe, Nasser, Tingrui Pei, and Moses Ntanda Kyebambe. "Application of deep learning for quality of service enhancement in internet of things: A review." Energies 14, no. 19 (2021): 6384.
[43] Akintaro, Mojolaoluwa, Teddy Pare, and Akalanka Mailewa Dissanayaka. "Darknet and black market activities against the cybersecurity: a survey." In The Midwest Instruction and Computing Symposium.(MICS), North Dakota State University, Fargo, ND. 2019.
[44] Babun, Leonardo, Kyle Denney, Z. Berkay Celik, Patrick McDaniel, and A. Selcuk Uluagac. "A survey on IoT platforms: Communication, security, and privacy perspectives." Computer Networks 192 (2021): 108040.
[45] Mlyatu, Maduhu Mshangi, and Camilius Sanga. "Secure web application technologies implementation through hardening security headers using automated threat modelling techniques." (2022).
[46] Fornero, Matteo, Nicolò Maunero, Paolo Prinetto, and Antonio Varriale. "SEkey: a distributed hardware-based key management system." In 2020 IEEE East-West Design & Test Symposium (EWDTS), pp. 1-7. IEEE, 2020.
[47] Mailewa, Akalanka, Jayantha Herath, and Susantha Herath. "A survey of effective and efficient software testing." In The Midwest Instruction and Computing Symposium (MICS), Grand Forks, ND. 2015.
[48] Ugale, Santosh, and Amol Potgantwar. "Container Security in Cloud Environments: A Comprehensive Analysis and Future Directions for DevSecOps." Engineering Proceedings 59, no. 1 (2023): 57.