5-2023

IOT Devices in Healthcare: Vulnerabilities, Threats and Mitigations

Isse Abdi

IOT Devices in Healthcare: Vulnerabilities, Threats and Mitigations

by

Isse Abdi

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

In Partial Fulfillment of the Requirements

For the Degree of

Master of Science in Information Assurance

May 2023

Starred paper Committee:
Akalanka B. Mailewa, Chairperson
Erich P. Rice
Mark B. Schmidt

Abstract

Internet of things has been a dream for many people in the beginning of the internet, today IOT devices are in every sector, healthcare being a major player because of the benefits as quality care for patients and easing the work for providers but on the other hand, it poses security threats to the patients and organizations, it is imperative to point out the best way to balance between the risks and opportunities that IOT creates for the sector; in this research, vulnerabilities and prior studies as well as ways to fix these weaknesses will be presented, it is also worth noting that due to the length of IOT vulnerabilities, the common ones will be discussed .

Table of Contents

Page

List of Tables

Table Page

List of Figures

Chapter I

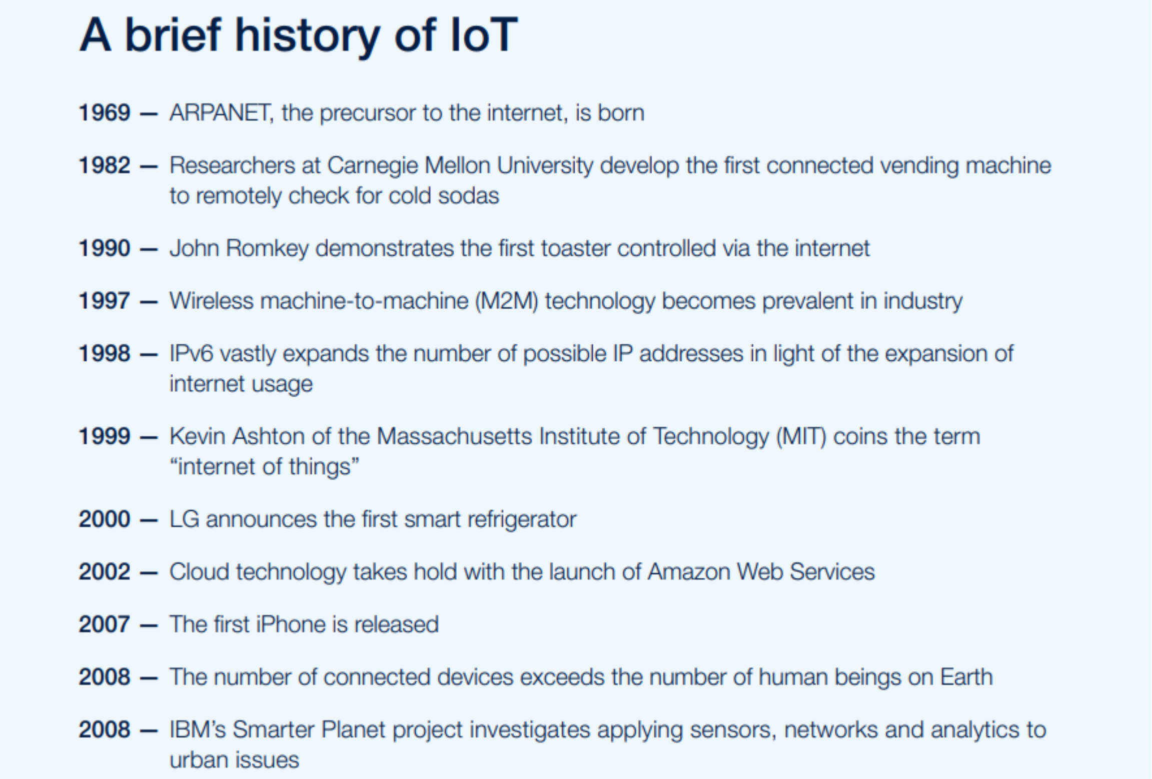
Introduction

Introduction

The term ‘Internet of Things’ was coined in 1999 by the computer scientist Kevin Ashton. While working at Procter & Gamble, Ashton proposed putting radio-frequency identification (RFID) chips on products to track them through a supply chain [1]. Internet of things have explored in the last years with the rise of internet usage in the world, one of the sectors that have seen a tangible increase is health care sector, it comprises from wearable devices that helps patient monitoring and disease tracking to imbedded systems. The Internet of Things (IoT) is a new technology that offers improvements and better solutions in the medical field, such as accurate medical record-keeping, sampling, device integration, and causes of illness [2]. However, with all benefits in place, there is an apparent risk comes with the devices connected to the internet, according to a 2020 special report by the ECRI Institute, when considering the top 10 health technology hazards, remote access was identified as the top technical risk in healthcare, which could interrupt the flow of data, alter or degrade the device’s performance, or expose protected health information. [3**]** Moreover, Researchers reported attacks such as eavesdropping on wireless communication or controlling other devices on insulin pumps and security breaches in implantable medical devices in order to alter the expected treatment [4]. to combat such tragedy from happening to patients, Health Insurance Portability and Accountability Act (HIPAA) have mandated technical safeguards to be in place for electronic protected health information (e-PHI), and many countries introduce similar acts and regulations. Compliance with such regulations, on the other hand, is now focused on audits and is rarely monitored on a continuous basis. One solution is to link data flowing through multi-layered, interconnected IoT healthcare systems to information about the safeguards in place. This could enhance audits by allowing for real-time compliance checks [5].

Historical background

Fig. 1. [6] State of the Connected World 2020 Edition INSIGHT REPORT DECEMBER 2020



A brief history of IoT

1969 — ARPANET, the precursor to the internet, is born

1982 — Researchers at Carnegie Mellon University develop the first connected vending machine to remotely check for cold sodas

1990 — John Romkey demonstrates the first toaster controlled via the internet

1997 — Wireless machine-to-machine (M2M) technology becomes prevalent in industry

1998 — IPv6 vastly expands the number of possible IP addresses in light of the expansion of internet usage

1999 — Kevin Ashton of the Massachusetts Institute of Technology (MIT) coins the term “internet of things”

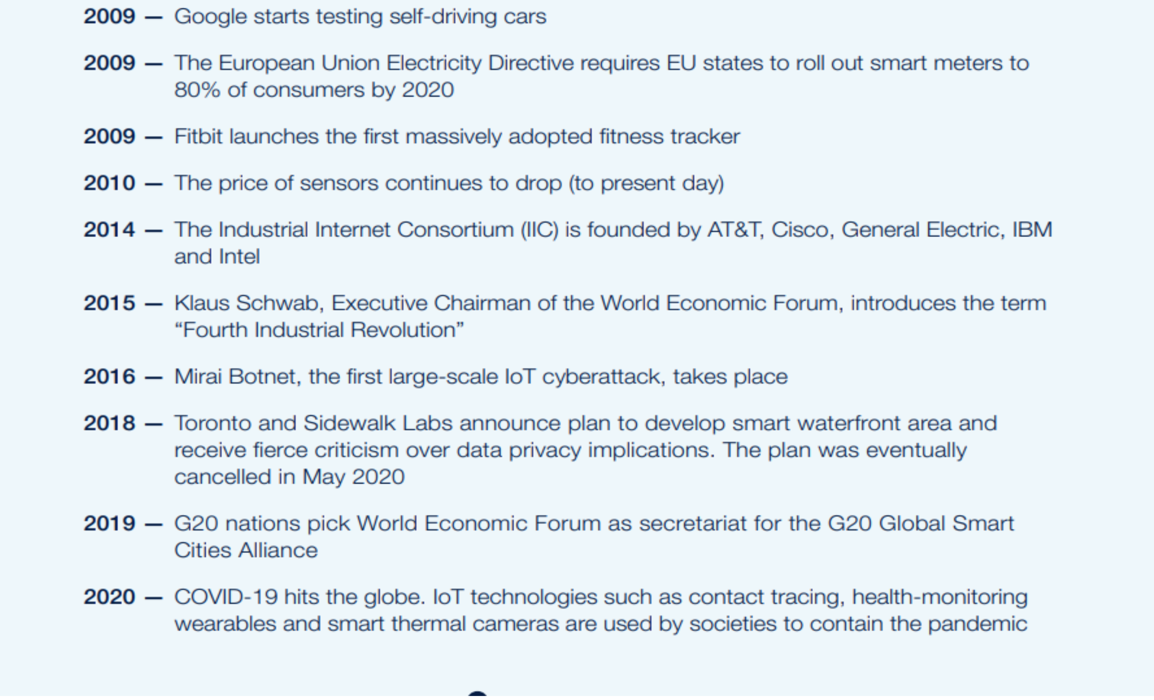
2000 — LG announces the first smart refrigerator

2002 — Cloud technology takes hold with the launch of Amazon Web Services

2007 — The first iPhone is released

2008 — The number of connected devices exceeds the number of human beings on Earth

2008 — IBM’s Smarter Planet project investigates applying sensors, networks and analytics to urban issues



2009 — Google starts testing self-driving cars

2009 — The European Union Electricity Directive requires EU states to roll out smart meters to 80% of consumers by 2020

2009 — Fitbit launches the first massively adopted fitness tracker

2010 — The price of sensors continues to drop (to present day)

2014 — The Industrial Internet Consortium (IIC) is founded by AT&T, Cisco, General Electric, IBM and Intel

2015 — Klaus Schwab, Executive Chairman of the World Economic Forum, introduces the term “Fourth Industrial Revolution”

2016 — Mirai Botnet, the first large-scale IoT cyberattack, takes place

2018 — Toronto and Sidewalk Labs announce plan to develop smart waterfront area and receive fierce criticism over data privacy implications. The plan was eventually cancelled in May 2020

2019 — G20 nations pick World Economic Forum as secretariat for the G20 Global Smart Cities Alliance

2020 — COVID-19 hits the globe. IoT technologies such as contact tracing, health-monitoring wearables and smart thermal cameras are used by societies to contain the pandemic

Problem Statement

Internet of things brought many benefits to the health care but at the same its downside stands out in the secuirty of these devices which would create more problem to the individual and organization level. IOT devices pose a great risk to the individual life and healthcare organization as bad actor can take control of oxygen monitoring machine and lower the oxygen level. Hackers can manipulate Pacemakers; they can play with Insulin pumps and increase/decrease the level, this can be a real threat that can result loss of life; on top of that, hackers can have access to patients’ private information and their Location.

Nature and Significance of the Problem

IOT security becomes imperative as the adaptations increases, the study shows

Objective of the survey that 80% of organizations experienced cyberattacks

on their IOT devices in 2018, and in 2019 eight in ten organizations have experienced a cyberattack on their IOT devices, of those organizations, 90% experienced an impact as a result of the cyberattack, including operational downtime and compromised customer data or end-user safety, However, the survey finds that 26% of the organizations did not use security protection technologies [7]. This is concerning data for healthcare providers and patients who are assessing the risk of exposing themselves to IoT devices. In 2018 At the RSA Conference USA, hackers "killed" (simulated) patients without the doctors even being aware that the operating room had been hacked [8]. The simulation was there to proof the seriousness of the matter that a patient who is undergoing surgery for life saving purpose or fixing of health related issue can die in the hands of caregivers due to IOT device vulnerabilities without the knowledge of healthcare providers in the room, the goal of the simulation was that healthcare providers should not only worry of the compliance of HIPPA but also the safety of their patients. What's more troubling is the medical devices such as pacemakers, implantable cardioverter defibrillators, insulin pumps, defibrillators, fetal monitors, and scanners are becoming more vulnerable and hospitals increasingly rely on these devices that communicate to one other, hospital medical record systems, and the Internet [9]. The impact of ambulance delays (due to rerouting around the marathon) on patient care, resulting in a statistically significant increase in 30-day mortality rates, was weighed in an article published in the New England Journal of Medicine of delays of emergency care and mortality during US Major Marathons [10]. The relevance of the data to this research is that, if people died due to an increase in the length of the ambulance ride, then it is highly possible and reasonable to die in the distributed denial of service attacks or any other attack that can disrupt a timely care delivery to those who need it; on top of that, the risks of OIT devices is accompanied by increased risk of patient privacy as these devices can enable unauthorized access and misuse of personal information. The fact is that privacy is challenging to understand and guarantee in a world where more and more smart devices collect data, share it, and monetize it [11]. Because IoT devices are producing significantly vast quantities of highly sensitive data, it is imperative that before building a smart healthcare system to consider numerous security and privacy concerns: the availability of all essential information when needed; effective and reliable surgical and diagnostic processes that help achieve this goal with a low error rate, high precision, and low cost; and access to internal and external resources as needed [12].

Objective of the Study

In the research, I would like to take the following approaches:

- Research IOT vulnerabilities and Threats in the healthcare sector.
- Study literature review and see what others have done to solve the issue.
- Describe the shortcoming of the previous efforts
- To see how existing regulations, certifications help to address those vulnerabilities
- Provide recommendations and mitigation techniques.

Study Questions/Hypotheses

The research is about vulnerabilities of IOT devices in healthcare sector and would like to answer the following research questions

- ➢ What role do IOT devices play in healthcare sector?
- ➢ What are the vulnerabilities and threats of these devices and the effects on individuals and organizations if compromised?
- ➢ What are the mitigations techniques of the threats?
- ➢ How can healthcare organizations balance the benefits and risks associated with IOT devices

Limitations of the Study

This research is intended to outline common vulnerabilities in Healthcare ITO devices and would not present all weakness in the devices or weakness of all devices that used in healthcare sector, the paper would brush off available research study in the field, and forward some of the mitigation techniques available. Since, the project is systematic literature review, no experiment was conducted to analyze the data collected.

Definition of Terms

IOT: internet of things

Vulnerabilities: any weakness that can be exploited by bad actor.

Threats: something that cause damage or harm.

Mitigations: reducing the overall risk or impact.

DOD: distributed denial of service attacks.

Hacker: a person uses his/her technical skills to gain access to data.

Pacemaker: a medical device implanted under a person's skin, with wiring going down to their heart and helps regulate abnormal heart rhythms.

ICD: (implantable cardioverter defibrillator) a battery-powered device placed under the skin that keeps track of your heart rate.

Shodan stands for Sentient Hyper-Optimised Data Access Network, it is a search engine designed to map and gather information about internet-connected devices and systems.

HIPAA: Health Insurance Portability and Accountability Act.

Summary

IOT devices are very common in the health care sector, it helps service delivery objective and improved patient results but on the other side brought extra burden on healthcare managers in terms of security and privacy, the aim of this research is to highlight weakness in those devices and explore ways to mitigate those risks, the solutions would be to balance the risks and benefits at the same time to achieve the desired goal.

Chapter II

Background and review of literature

Introduction

The discussion in this chapter would be around the background of the research problem by addressing the tangible effects of the research problem to humans and assets to show the importance of addressing the issue and the need for the sustainable solution as well as the reviewing the previous writings related to the problem and methodology.

Background Related to the Problem

Nowadays Internet of Things (IoT) is widely adopted in many applications that its importance is extending in our daily life. The IoT technology is also developing in the healthcare monitoring system for providing effective emergency services to patients [13]. Internet of things devices help healthcare sector in many ways, like monitoring patients and even protecting other medical devices and figuring out their real time locations when needed, for example wheelchairs and oxygen pumps but with all the benefits comes at a cost of risking patient information and even their safety if not well safeguarded, there are potentially significant concerns associated with the Internet of Things. Boundaries erode or become harder to establish and protect when there are so many interconnected things. The weaknesses of systems become increasingly serious as they get more intertwined, interdependent, and sophisticated. Any interruption or corruption in critical systems could result in property damage or, in the worst-case scenario, death. However, concerns about security, privacy, and user interface standardization are increasingly important [14].

While IoTs has many advantages, it also brings with it an increased risk of security breaches and vulnerabilities in medical systems. It's for these reasons why this has happened:

Patients' vital information is the primary goal of clinical instruments, which are used to acquire and communicate data; the IoTs phenomena produces inconsistencies and complexities; and medical IoTs device producers disregard security considerations. The aforementioned considerations have led to an increase in the number of people worried about the Confidentiality, Integrity, and Accessibility (CIA) of information. Examples of IoTs applications in medical include programs and equipment that monitor and manage an individual's vital signs. Although these techniques may be exposed to security issues e.g., privacy, authorization and verification threats. Cybersecurity has become a big issue in the medical business. Device weaknesses might be used by hackers to compromise the IoTs framework. When it comes to resolving attacks, standard security standards are irrelevant because of the limitations of medical technology [15]. IoT medical sensors are meant to collect data on a patient's status in real time, and hospitals receive this information to help their patients as part of their healthcare monitoring and data analysis. However, because IoT-based healthcare infrastructure is integrated with traditional IT infrastructure and operations, new risks may arise. Along with its unclear set of functionalities, the Internet of Things as an Emerging Technology will face numerous security issues. [16]. The underlying problem here is that even though IOT devices' known weakness, they are also connected or impeded into other IT systems and if the IOT device's vulnerability is exploited, the impact will touch other systems and same time, the challenge expands to the little solutions available to solve the problem.

The health-care dilemma is that, most IoT devices and other healthcare services rely on wireless networks such as WI-FI, which are considered to be potential targets for attackers due to their simplicity, high availability, and low cost. On the other hand, the majority of IoT Healthcare devices are internet connected. A smart wearable temperature sensor or heart monitor which is connected to the internet, for example, can alert the caregiver based on the patient's status. When the user is at home, the wearables are connected to the home network, and when he or she is at work, they are connected to the office network. Certain sensor devices are, in general, very mobile. On of that, Various network configurations and security settings exist in the field. As a result, creating a secure algorithm that is also mobile is a significant challenge [17].

Literature Related to the Problem

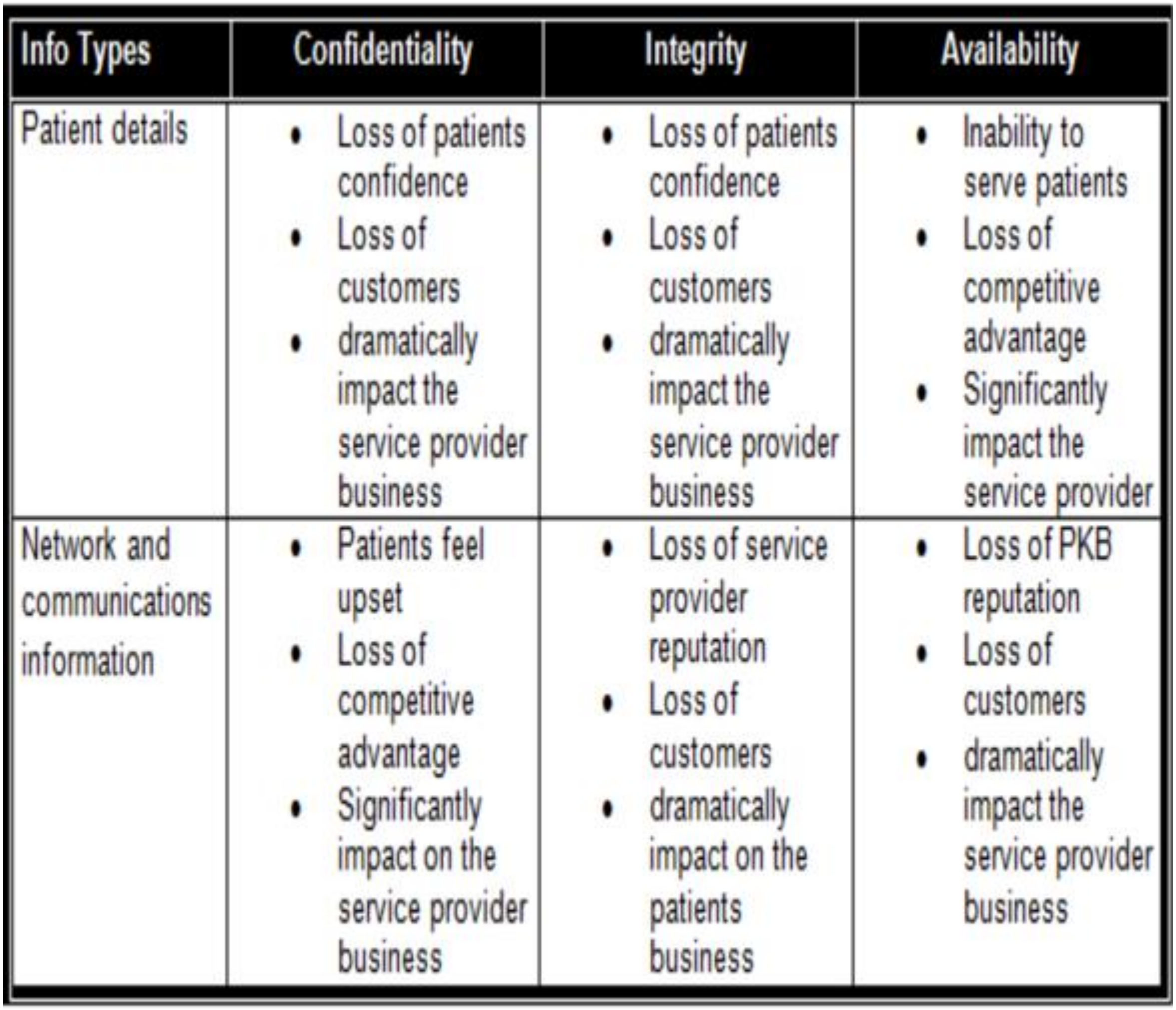
The problem presented here refers to what other researchers have discovered pertaining to IOT vulnerabilities whether it is a real incident that took place or weakness exposed by security analyst. In general, cyberattacks have seen an increase of 125% in the healthcare ecosystems within the last 5 years [18]. In late 2015, two security researchers discovered over 68,000 medical systems that were exposed online, and 12,000 of them belonged to one healthcare organization [19]. The numbers, represent the threat level of IOT devices and risks associated with it if compromised by bad actors who can disrupt the system operation and take personal information as a hostage.

A number of research contribution has been invested to expose healthcare IOT vulnerabilities so that venders and healthcare providers can mitigate these risks promptly, and the fact that these devices are connected to the Internet via computers running relatively old versions of Windows XP, a version of the OS known to have numerous exploitable flaws, is one of the key concerns surrounding their discovery. Shodan, a search engine that can find IoT devices online that are connected to the internet, was used to find these devices. Using brute-force attacks and hard-coded logins, these are simple to break into. Using simple Shodan queries, two experts were able to find anesthetic equipment, cardiology devices, nuclear medical systems, infusion systems, pacemakers, MRI scanners, and other devices [20]. The threat is so scary as these critical systems are accessible through an online publically available search engine that even low skilled hackers like script kiddies can take advantage and cause damage to the sector and users as well. In comparison to other industries, the healthcare sector has particular vulnerabilities. This is related to the connectivity of various medical devices with other components of the network, as well as the lack of security mechanisms on these medical devices in general. The healthcare information infrastructure has a huge number of old systems that are difficult to update, and threat actors are constantly probing this system for vulnerabilities. Potential breaches of critical patient data, such as personal and financial information, could provide further benefits to cybercriminals or internal attackers [21], and in this digital era, the healthcare sector has shown to be particularly vulnerable, and it is one of the most common targets for hackers. This is because attacking healthcare is a low-risk, high-reward crime, and the Covid-19 outbreak has exposed just how vulnerable and unprepared healthcare systems are, posing a serious threat to global health [22].

on the other hand, other researchers have taken deeply into what if these devices are compromised and presented the level of impact for healthcare community, the impact is measured with CIA triad and was drawn from two sides, patient information and network or communication side, the level of impact to the patients and healthcare providers could range from low to high impact. This is a step forward for healthcare providers to prepare for the tragedy and put remedial mechanism in place; the table below summarizes the level impact based on loss of confidentiality, integrity and availability model.

Table 1.

[23] Internet of Things Security: A Review of Risks and Threats to Healthcare Sector (2017)



Info Types	Confidentiality	Integrity	Availability
Patient details	• Loss of patients confidence • Loss of customers • dramatically impact the service provider business	• Loss of patients confidence • Loss of customers • dramatically impact the service provider business	• Inability to serve patients • Loss of competitive advantage • Significantly impact the service provider
Network and communications information	• Patients feel upset • Loss of competitive advantage • Significantly impact on the service provider business	• Loss of service provider reputation • Loss of customers • dramatically impact on the patients business	• Loss of PKB reputation • Loss of customers • dramatically impact the service provider business

The examples given above, show the level of vulnerability for Internet of things in healthcare and how it is easily accessible for bad actors, also the level of impact supersedes everything to the extent of loss of human life. The challenge is not only coming from hackers but the nature of the IOT devices is complex and designing a standard framework to secure it would be difficult.

Literature Related to the Methodology

Internet of things in healthcare sector received the attention of researchers and a lot has been written about it due to its rapid changes and adaptations ; Safazi, Sayidmustafa and other researchers [24] investigated Cyber Vulnerabilities in Smart Healthcare, The authors' contribution to the subject is the review the weakness of IOT devices and presented some solutions and mitigation techniques, they presented how smart homes and healthcare have become increasingly popular In recent years and because of the volume of data transmitted , it requires the use of a more secure way to assure security and privacy; but to my view point, their work serves as a general approach of all IOT devices in the field and it lacks the focus of IOT vulnerabilities in healthcare, their topic seems to be dealing with smart healthcare but rather switched to smart homes, another shortcoming in this research, they have not presented real example of incidents that effected healthcare sector.

The second literature reviewed in this methodology is presented by group of authors, Zubair et al, [25] their research is titled “Exploiting Bluetooth Vulnerabilities In e-health IOT Devices” the researchers presented the role that Bluetooth technology plays in communication in today's interconnected world because of its low resource consumption, which is ideal for IoT architecture and design and since Bluetooth technology, on the other hand, is not without security issues they have done thorough investigation on attacks on IOT devices that connect in short range wireless through radio frequency, they presented various attack scenarios for these devices and the need to implement measures for protecting healthcare data while implementing Bluetooth enabled devices ; even though the research fits its topic but it is only focusing on one part of the problem, and that is to say that not all IOT devices in healthcare connect through

Bluetooth and sometimes the need for far range wireless monitoring devices may be more than the need for short range ones.

The 3rd literature reviewed in this paper is contributed by Zakaria, H and others,[26] their research is about IoT Security Risk Management Model for Secured Practice in the Healthcare Environment, they explained that the emergence of Internet of Things (IoT) technology for unified and networked medical devices and sensors has altered the healthcare industry's landscape with the 'openness' of the distributed environment and medical devices, they further predicted that IoT is the point of a breach and allows attackers to pinpoint vulnerabilities and start attacks. This poses a considerable risk to the hospital environment, potentially jeopardizing its security measures. From the reading of their research, it is well written in the subject matter and addresses ways to overcome security flaws of IOT healthcare devices but their study is based on a Malaysian hospital and not for general healthcare environment.

The 4th literature reviewed in this research is written by Zhou, W and others [27], who looked at IoT security, privacy and features. They highlighted the security risks, known solutions, and unsolved research issues connected with certain IoT capabilities. They also pointed out which innovative security technologies need more research. They showed some of the development patterns of recent IoT security research and how IoT features reflect on existing research based on assessing a large amount of valuable research. The authors' contribution seems to be so important but their topics is for IOT devices in general and not specific to the healthcare sector, also their research seems to be audited and a lot changed since then.

Summary

In this chapter, we discussed the background of the IOT devices in healthcare, the real problem was presented that was drawn from the previous writings and the short falls in their research area which takes the vital point of more research in devices of healthcare providers to protect and serve patients in the best manner.

Chapter III

Methodology

Introduction

In this chapter, the methodology of the research will be presented composing design, data collected, tools, and progress and time line of the research

Design of the Study

The framework of this study would focus on IT devices in the health care sector, vulnerabilities, threats and mitigation techniques, we will also illustrate how the existing tools would help the sector to protect their systems and thwart possible attacks, both qualitative and quantitative would be used as the research and to study the research problem approach.

Data Collection

In this part of the research, we will put compromised data, listing the attacks that happened on IOT devices and the kind weakness that caused the threat. This would not be all data on every IOT device but a sample table acting as a summary, because of the large amount of data collected, stored, and processed by Healthcare IOT-based devices, data security is becoming increasingly important. This information can be customized, location-specific, or patient-centric, depending on the nature of the device [28].

In MITRE common weakness enumeration shows some vulnerabilities for Healthcare IOT devices that cause significant damage to the organization [29].

Table 2

(21) CWE-1357: Reliance on Uncontrolled Component.

CWE 1329	Issue	Description	Scope	Impact	Example
	Reliance on Component That is Not Updateable	The product contains a component that cannot be updated or patched in order to remove vulnerabilities or significant bugs	Confidentiality Integrity Access Control Authentication Authorization Other	**Technical Impact:** *Gain Privileges or Assume Identity; Bypass Protection Mechanism; Execute Unauthorized Code or Commands; DoS: Crash, Exit, or Restart; Quality Degradation; Reduce Maintainability* If an attacker can identify an exploitable vulnerability in one product that has no means of patching, the attack may be used against all affected versions of that product.	A refrigerator has an Internet interface for the official purpose of alerting the manufacturer when that refrigerator detects a fault. Because the device is attached to the Internet, the refrigerator is a target for hackers who may wish to use the device other potentially more nefarious purposes

Tools and Techniques

The techniques used in this research paper is mainly identifying vulnerabilities for IOT devices, threats that can exploit those vulnerabilities and ways to protect it

Hardware and Software Environment

Hardware and service components make up healthcare IoT devices. The hardware component allows the entity to connect with objects and processes in the digital domain, while the service provides a well-defined and standardized interface with all necessary features. By accessing a device's hosted resource, the services reveal its functionality [30]. The hardware is the device itself that the entity like humans or software agents use it to communicate. In other words, IOT hardware is the device and the software is what making them connect or be impeded into other devices.

The IoT devices range from extremely small sensors driven by 8-bit microcontrollers (MCUs) to more powerful but energy-efficient 32-bit processors. Different architectures are used in these devices, including x86, MSP430, ARM7, Atmel AVR, Cortex-M0, Cortex-M3, and Cortex-M4. An IoT OS should be able to run on a variety of platforms, including embedded devices and standard PCs, and support multiple drivers and interfaces [31]. These devices have no space and power constraints and are comparable to regular PCs. Similarly, to software, malicious hardware circuits can be placed on the medical device itself, but also on other devices it communicates with, i.e., the programming device and the home device in our pacemaker scenario. Malicious hardware on the web server, where pacemaker data are stored, also poses a threat by either revealing sensitive medical data or by even modifying these data and, thus, misleading the treating physician [32].

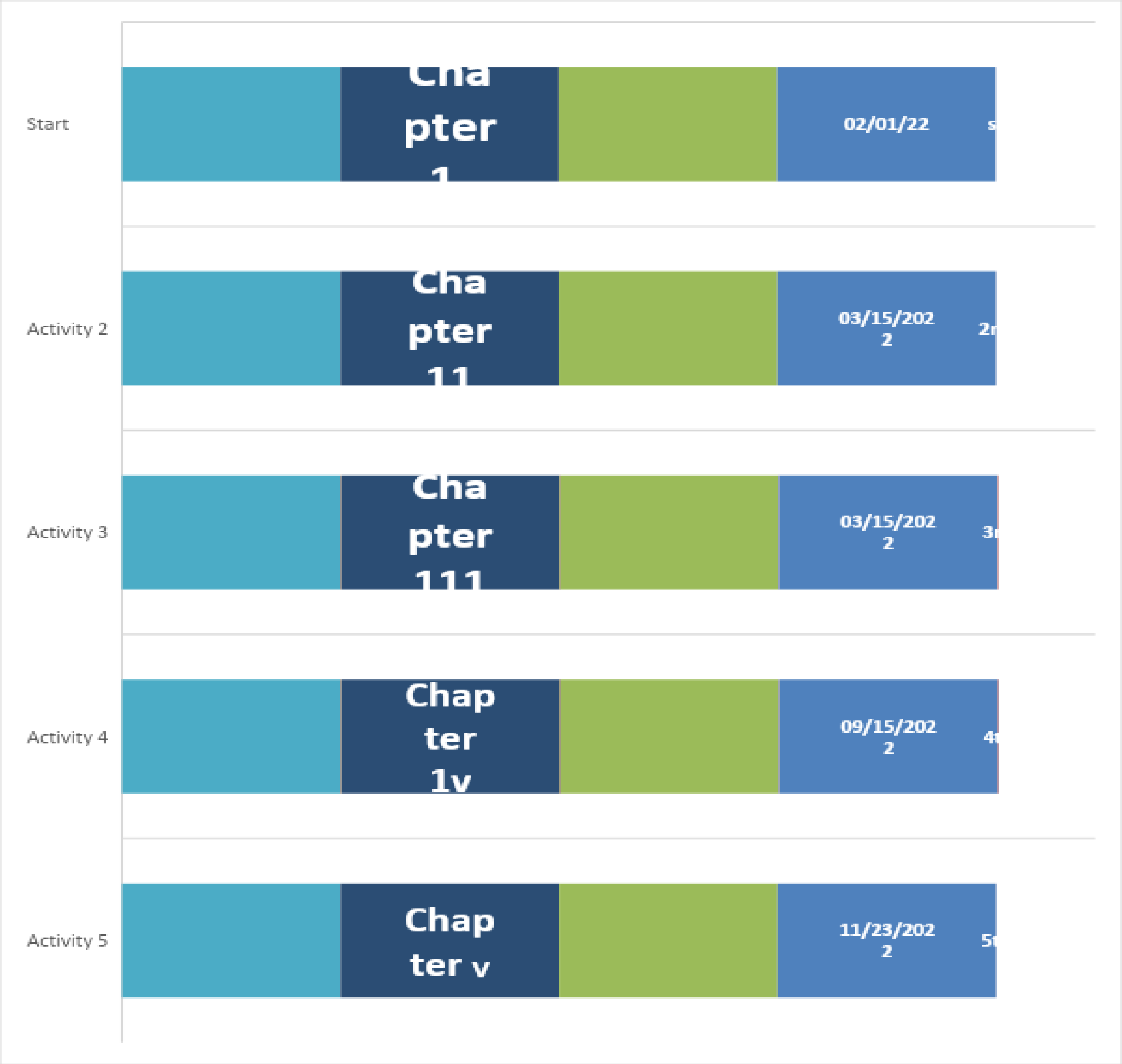
Work in progress

This project is for starred paper to fulfill the requirement of acquiring Master’s degree in information assurance, it started with the project proposal, where the work progress have been slowly moving, in the beginning, three parts are completed, chapter one is for the introduction, chapter two for the background and literature review and chapter three for the research methodology. In the second term, another two chapters are completed, chapter four for Data Presentation and Analysis and chapter five for Results, Conclusion, and Recommendations.

Timeline

This timeline is for the completion of the project proposal, project final draft series 1,2 for chapters one to five. We have used Microsoft Study software to develop a Gantt chart.

Fig. 2. (23) Project Time Line



Summary

Reviewing collected data and looking MITRE's common vulnerabilities would support healthcare leaders and venders to take necessary precautions before introducing software designs or deploying in the systems.

Chapter IV:

Data Presentation and Analysis

Introduction

In this part of the research, the focus would be to outline the collected data by simplifying and explaining the best way to use in the field

Data Presentation

According to Cynerio's 2022 State of Healthcare IoT Device Security research, more than half of Internet of Things (IoT) devices used in hospitals have serious cybersecurity flaws. Hospital data, patients, and individuals who depend on IoT devices can all be at risk due to security flaws in healthcare settings. According to a framework based on the NIST Cybersecurity Framework, the research lists the top cyber risks that hospital IoT devices are most vulnerable to, along with the devices that are most at risk. These are the top five devices with high risk levels [33]:

- IV pump.
- Voice over Internet Protocol (VoIP) phone.
- Ultrasound.
- Medicine dispenser.
- IP camera

Data Analysis

To address the growing concern of cybersecurity in medical devices, the Food and Drug Administration (FDA) has created cybersecurity guidelines for three medical device classes (table 1) before devices are introduced to the market [34].

Table 3

[26]. Medical device classes

Medical Device Class	Attributes	Example Devices
Class I	Common, low risk, low complexity	Lancet, Dental Floss
Class II	More complex, greater risk to patient, partially implanted	Syringe, Insulin Pump, BGM
Class III	Fully implanted, greater risk, regulate body functions Replacement Heart Valves	Artificial Pancreas, CGM,

The main concern as mentioned above, comes from medical devices that are in the second and third class, it poses health risks and even death if used in the wrong way.

Summary

In this chapter, we discussed the available data to show the severity of the problem, the data explained the kind of threat that devices have irrespectively, in the analysis of data, what stood out was the need for security experts and healthcare leaders to prioritize their focus in securing devices in the 3r and 2nd classes.

Chapter V:

Results, Conclusion, and Recommendations

Introduction

In the last chapter of the paper, the results the of the research is presented, answering study questions, concluding the research paper content and putting down future work recommendations.

Results

The research is about vulnerabilities of IOT devices in healthcare sector and answered the following research questions

What role do IOT devices play in healthcare sector?

Based on the research it is clear that IOT devices play remarkable role in the healthcare sector. The impact of the Internet of Things (IoT) on the advancement of the healthcare industry is immense. The ushering of the Medicine 4.0(predictive, preventative, personalized, and participatory) has resulted in an increased effort to develop platforms, both at the hardware level as well as the underlying software level. This vision has led to the development of Healthcare IoT (H-IoT) systems [35]. IoT has had a positive impact on e-health, assisted living, human-centric sensing and wellness. Recently this interconnection has been referred to as Healthcare IoT (H-IoT). Real-time monitoring based on the information gathered from the connected ‘things’ provides large scale connectivity and a greater insight into patient care, individual habits and routines [36]. Therefore, it is clear that IOT devices help both providers and patients to promote a sustainable healthy atmosphere.

What are the vulnerabilities and threats of these devices and the effects on individuals and organizations if compromised?

As discussed in previous chapters, while IOT devices bring uncountable benefits to the health care industry, it has devastating vulnerabilities that should be addressed appropriately. As more devices enter the realm of the IoT, data attacks aimed at the diversity of new Internet-connected endpoints will inevitably become more common. Whereas developers see in Internet-connected devices a wealth of new capability, attackers see a vast new attack surface [37]. While healthcare IOT devices face similar secuirty challenges as any other devices but there are challenges unique to them. The security problems in IoT are different from the security problems on the internet (World Wide Web). IoT security issues are privacy, authorization, verification, access control, system configuration, information storage, and management. The recent tends about a secure architecture for smart cities, security protocol, lightweight cryptography, lightweight authentication, the blockchain, and data privacy preserving [38].

What are the mitigations techniques of the threats?

Practically speaking, there are no bullet proof techniques for threat modeling of H-IOT devices but the general security concept of CIA secuirty triad must be applied as well as other device specific defense mechanisms; including hanging default passwords, device/system authentication, strict firewall rules, static code analysis (SCA) executed within the IoT system or applications and network intrusion detection mechanisms. Authentication of all connected IoT devices is a mitigation method used to reduce the likelihood of malicious devices infiltrating the network [39].

How can healthcare organizations balance the benefits and risks associated with IOT devices?

Answering this study questions is the most important part of the research paper, it seems to be a multi-million question, simply because, the goal of the study was not scary users and sway them away from using the devices rather to balance the benefits and risks associated with it. The balance would start H-IOT as an interconnected systems of architecture that need frameworks and metrics to safeguard rather a single device. An integration of IoT risk vertices into reliable cyber security frameworks would help with preventing abuse originating from malicious interventions, including those perpetrated by organized crime, terror organizations or state-sponsored aggressors [40].

Conclusion

Healthcare IOT devices contributed improving patients' wellbeings and eased the work for healthcare providers. Remote monitoring and producing valuable data for patients help clinical doctors to make effective decisions for their patients, but at the same, the devices are bringing unprecedented risks to the patients and healthcare systems. For patients, the risk can be PPI exposure or even death, and for healthcare systems, loss of data, services interruption, and damage to the infrastructure reputation as well fines; therefore, securing medical devices means protecting human life, human health, and human well-being. It is imperative that health care leaders must focus address those vulnerabilities and put appropriate controls in place.

Future Work

Future research in health care IOT devices should solve underlying security flaws to protect patients' personal protected information from falling in the wrong hands, an important solution would be to use cryptographic algorithms to provide confidentiality and integrity of the transmitted data between the sender and receiver [41].

Similarly, the security of healthcare IoT will be bolstered by advances in cryptographic technologies, e.g. blockchain [42]. Future work should also concentrate on creating more durable and dependable technologies that can scale well, use less energy, and are simple to integrate into healthcare systems. They should address scalability, privacy, and security.

References

[1] M. Ben-Daya et al., “Internet of things and supply chain management: A literature review,” *Int. J. Prod. Res.*, vol. 57, no. 15-16, pp. 4719-4742, 2019. doi:10.1080/00207543.2017.1402140.

[2] M. Javaid and I. H. Khan, “Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic,” *J. Oral Biol. Craniofac, Res.*, vol. 11, no. 2, pp. 209-214, 2021. doi:10.1016/j.jobcr.2021.01.015.

[3] E. Brief, “Top 10 Health Technology Hazards for 2020.” ECRI Inst., 2019, p. 9.

[4] X. Hei et al., PIPAC: Patient Infusion Pattern based Access Control Scheme for Wireless Insulin Pump System v2. 9.

[6] World Economic Forum - Home.” https://www3.weforum.org/docs, The_State_of_the_Connected_World_2020.pdf. https://cwe.mitre.org/accessed 05-25-22023.

[7] New 2019 “Global survey: IoT- Focused cyberattacks are the new normal. (n.d.)”. Available at: https://resources.irdeto.com/global-connected-industries-cybersecurity-survey/new-2019-global-survey-iot-focused-cyberattacks-are-the-new-normal.

[8] “Healthcare and cybersecurity,” *Highlights RSAC*. RSA Conference. Available at: https://www.rsaconference.com/library/video/healthcare-and-cybersecurity-highlights-from-rsac-2018, 2018. (20201108T040602Z).

[9] A. Chacko and T. Hayajneh “Security and privacy issues with IoT in healthcare,” *EAI Endorsed Trans. Pervasive Health Technol.*, vol. 0, no. 0, p. 155079, 2018. doi:10.4108/eai.13-7-2018.155079.

[10] A. B. Jena et al., “Delays in emergency care and mortality during major U.S. marathons,” *N. Engl. J. Med.*, vol. 376, no. 15, pp. 1441-1450, 2017. doi:10.1056/NEJMsa1614073.

[11] K. Fu et al., 2020 Safety, security, and privacy threats posed by accelerating trends in the internet of things. arXiv preprint arXiv:2008.00017.

[12] A. Algarni “A survey and classification of security and privacy research in smart healthcare systems,” *IEEE Access*, vol. 7, 101879-101894, 2019. doi:10.1109/ACCESS.2019.2930962.

[13] M. Poongodi et al., “Smart healthcare in smart cities: Wireless patient monitoring system using IoT,” *J. Supercomput.*, vol. 77, no. 11, pp. 12230-12255, 2021. doi:10.1007/s11227-021-03765-w.

[14] A. M. Rahmani et al., “Exploiting smart e-health gateways at the edge of healthcare Internet-of-Things: A fog computing approach,” *Future Gener. Comput. Syst*, vol. 78, pp. 641-658, 2018. doi:10.1016/j.future.2017.02.014.

[15] R. Want and S. Dustdar "Activating the Internet of things [Guest editors' introduction]," *Computer*, vol. 48, no. 9, pp. 16-20, 2015. doi:10.1109/MC.2015.282.

[16] L. Jiang "IoT Sensors for Smart Health Devices and Data security in Healthcare," *J. J. Biomed. Sustain. Healthc. Appl.*, pp. 105-112, 2021. doi:10.53759/0088/JBSHA202101013.

[17] N. S. Abouzakhar et al., "Internet of things security: A review of risks and threats to healthcare sector," vol. 2017, pp. 373-378, 2017. doi:10.1109/iThings-GreenCom-CPSCom-SmartData.2017.62.

[18] N. N. Thilakarathne et al., "The role of the Internet of things in health care: A systematic and comprehensive study. *International Journal of Engineering and Management Research*, vol. 10, no. 4, p. 16, 2020.

[19] K. Kioskli et al., "The landscape of cybersecurity vulnerabilities and challenges in healthcare: Security standards and paradigm shift recommendations". The 16th International Conference on Availability, Reliability and Security, 1-9, 2021. doi:10.1145/3465481.3470033.

[20] Sciforce. 2019, Mar. 18 "Guaranteeing privacy and security in the healthcare IoT. Sciforce. Available at: https://medium.com/sciforce/ensuring-privacy-and-security-in-the-healthcare-iot-7b97549d629c.

[21] A. Chacko and T. Hayajneh. "Security and privacy issues with IoT in healthcare," *EAI Endorsed Trans.Pervasive Health Technol*, vol. 0, no. 0, p. 155079, 2018. doi:10.4108/eai.13-7-2018.155079.

[22] S. Islam et al., "Cyberattack path generation and prioritization for securing healthcare systems," *Appl. Sci.*, vol. 12, no. 9, p. 4443, 2022. doi:10.3390/app12094443.

[23] K. Kioskli et al., "The landscape of cybersecurity vulnerabilities and challenges in healthcare: Security standards and paradigm shift recommendations". The 16th International Conference on Availability, Reliability and Security, 1-9, 2021. doi:10.1145/3465481.3470033.

[24] N. S. Abouzakhar et al., Internet of things security: A review of risks and threats to healthcare sector," *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data*, vol. 2017, pp. 373-378, 2017. doi:10.1109/iThings-GreenCom-CPSCom-SmartData.2017.62.

[25] S. Safavi et al., "Cyber vulnerabilities on smart healthcare, review and solutions" Cyber Resilience Conference, vol. 2018. CRC, 2018, pp. 1-5. doi:10.1109/CR.2018.8626826.

[26] M. Zubair et al., "Exploiting Bluetooth vulnerabilities in e-health IoT devices" in *Proc. 3rd International Conference on Future Networks and Distributed Systems*, 2019, Jul., pp. 1-7. doi:10.1145/3341325.3342000.

[27] H. Zakaria et al., “IoT security risk management model for secured practice in healthcare environment” *Procedia Comput Sci*, vol. 161, pp. 1241-1248, 2019. doi:10.1016/j.procs.2019.11.238.

[28] W. Zhou et al., “The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved,” *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1606-1616, 2018. doi:10.1109/JIOT.2018.2847733.

[29] M. Harz et al., “A novel workflow-centric breast MRI reading prototype utilizing multitouch gestures” in *Breast Imaging* 11th international workshop], *Proc. 11*. Philadelphia, PA, USA: IWDM, July 8-11, 2012. Berlin Heidelberg: Springer, 2012, pp. 276-283.

[30] CWE - Common Weakness Enumeration.” https://cwe.mitre.org/accessed 05-25-22023

[31] J. Laassiri and S. Krit. “Internet of Things—Architecture and concepts in ODP information language” International Conference on Engineering & MIS (ICEMIS), vol. 2016, 2016, pp. 1-5. doi:10.1109/ICEMIS.2016.7745336.

[32] G. Gardašević et al., “The IoT architectural framework, design issues and application domains,” *Wirel. Personal Common.* vol. 92, no. 1. pp. 127-148, 2017. doi:10.1007/s11277-016-3842-3.

[33] J. Sametinger et al., “Security challenges for medical devices,” *Common.ACM*, vol. 58, no. 4, pp. 74-82, 2015. doi:10.1145/2667218.

[34] Cynerio, “The State of Healthcare IoT Device Security. 2022 https://www.securitymagazine.com/articles/97065-53-of-hospital-iot-devices-have-security-vulnerabilities,” vol. 11:10, p. 56, 2022-10-21.

[35] E. McMahon et al., “Assessing medical device vulnerabilities on the Internet of Things” in IEEE international conference on intelligence and security informatics (ISI), vol. 2017. IEEE, 2017, Jul., pp. 176-178. doi:10.1109/ISI.2017.8004903.

[36] Y. A. Qadri et al., “The future of healthcare internet of things: A survey of emerging technologies,” *IEEE Commun. Surv. Tutor.*, vol. 22, no. 2, pp. 1121-1167, 2020. doi:10.1109/COMST.2020.2973314.

[37] M. O’Neill “The Internet of Things: Do more devices mean more risks?,” *Comput. Fraud Sec*, vol. 2014, no. 1, pp. 16-17, 2014. doi:10.1016/S1361-3723(14)70008-9.

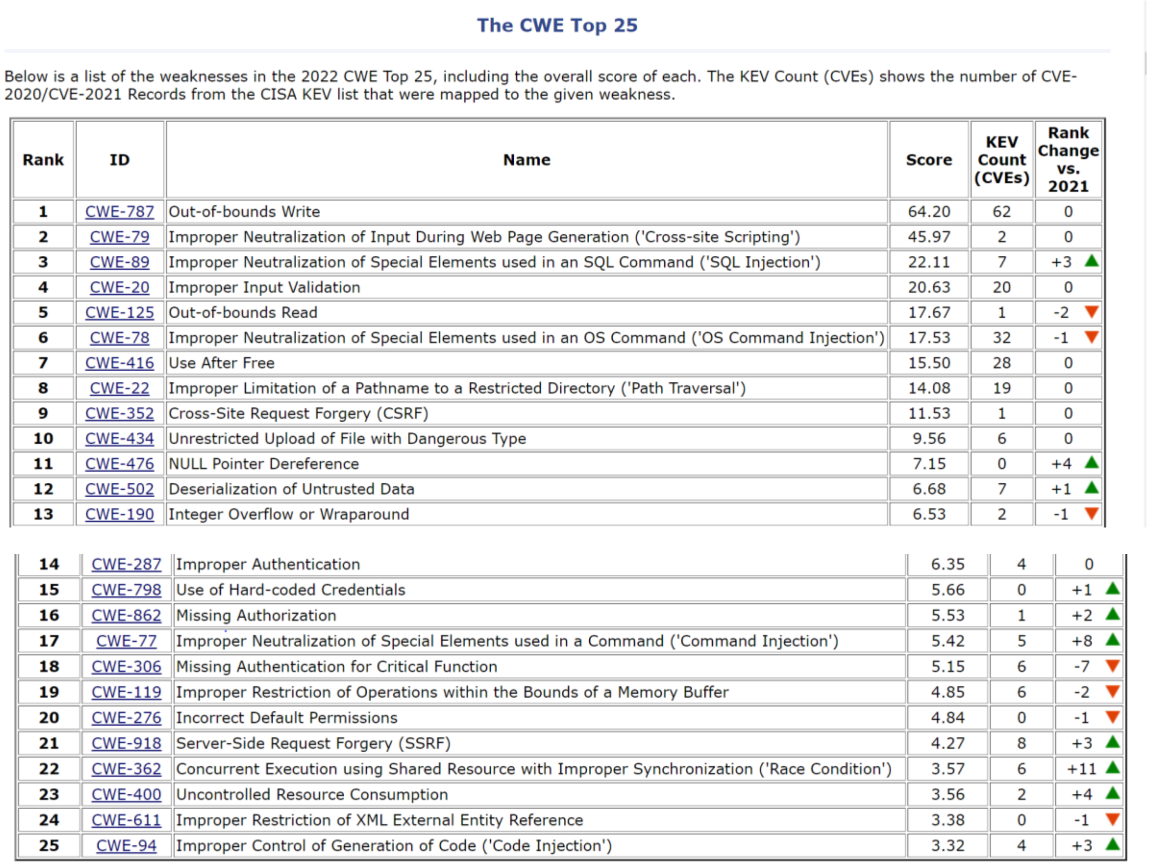
[38] D. Puthal et al., “The blockchain as a decentralized security framework [future directions],” *IEEE Con. Electron. Mag.*, vol. 7, no. 2, pp. 18-21, 2018. doi:10.1109/MCE.2017.2776459.

[39] R. Ande et al., “Internet of Things: Evolution and technologies from a security perspective,” *Sustain. Cities Soc.*, vol. 54, p. 101728, 2020. doi:10.1016/j.scs.2019.101728.

[40] P. Radanliev et al., “Future developments in cyber risk assessment for the internet of things,” *Comput. Ind.*, vol. 102, pp. 14-22, 2018. doi:10.1016/j.compind.2018.08.002.

Appendix A: Top 25 Common Weakness Enumeration 2022 List

Table .4[43] the CWE Top 25



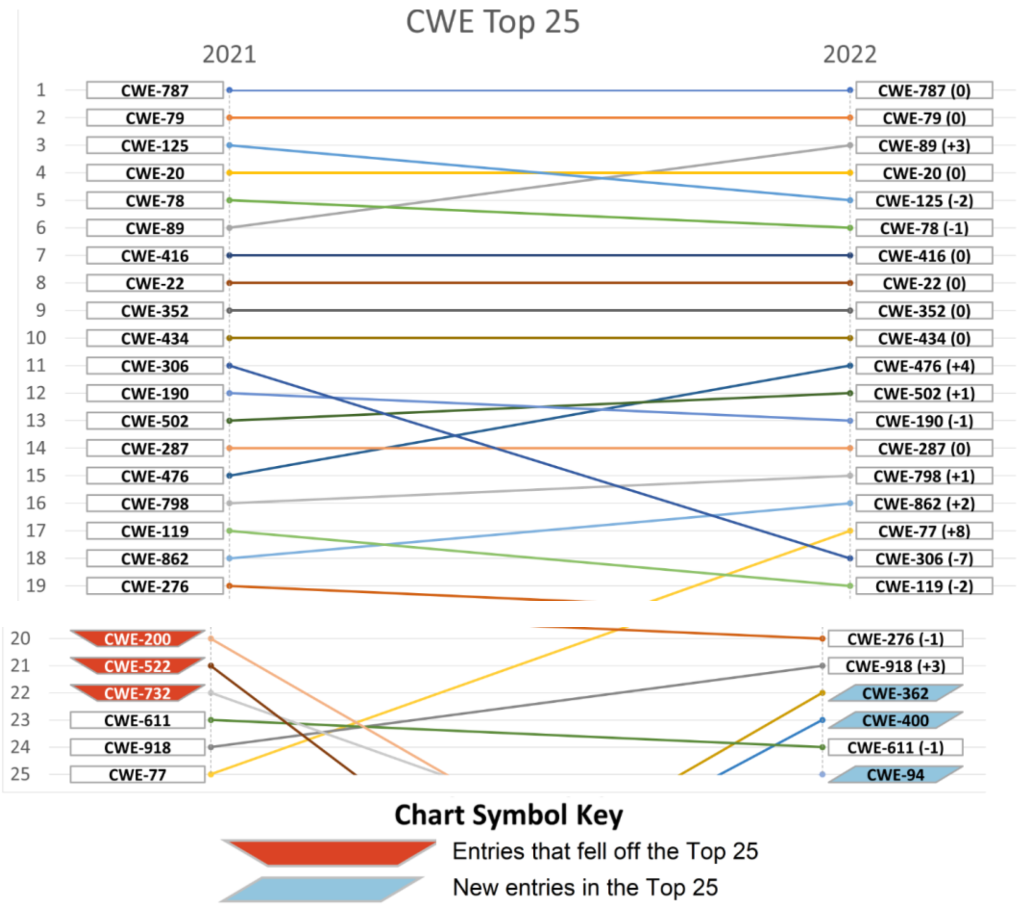
The CWE Top 25

Below is a list of the weaknesses in the 2022 CWE Top 25, including the overall score of each. The KEV Count (CVEs) shows the number of CVE-2020/CVE-2021 Records from the CISA KEV list that were mapped to the given weakness.

Rank	ID	Name	Score	KEV Count (CVEs)	Rank Change vs. 2021
1	CWE-787	Out-of-bounds Write	64.20	62	0
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.97	2	0
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22.11	7	+3 ▲
4	CWE-20	Improper Input Validation	20.63	20	0
5	CWE-125	Out-of-bounds Read	17.67	1	-2 ▼
6	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17.53	32	-1 ▼
7	CWE-416	Use After Free	15.50	28	0
8	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.08	19	0
9	CWE-352	Cross-Site Request Forgery (CSRF)	11.53	1	0
10	CWE-434	Unrestricted Upload of File with Dangerous Type	9.56	6	0
11	CWE-476	NULL Pointer Dereference	7.15	0	+4 ▲
12	CWE-502	Deserialization of Untrusted Data	6.68	7	+1 ▲
13	CWE-190	Integer Overflow or Wraparound	6.53	2	-1 ▼
14	CWE-287	Improper Authentication	6.35	4	0
15	CWE-798	Use of Hard-coded Credentials	5.66	0	+1 ▲
16	CWE-862	Missing Authorization	5.53	1	+2 ▲
17	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	5.42	5	+8 ▲
18	CWE-306	Missing Authentication for Critical Function	5.15	6	-7 ▼
19	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	4.85	6	-2 ▼
20	CWE-276	Incorrect Default Permissions	4.84	0	-1 ▼
21	CWE-918	Server-Side Request Forgery (SSRF)	4.27	8	+3 ▲
22	CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	3.57	6	+11 ▲
23	CWE-400	Uncontrolled Resource Consumption	3.56	2	+4 ▲
24	CWE-611	Improper Restriction of XML External Entity Reference	3.38	0	-1 ▼
25	CWE-94	Improper Control of Generation of Code ('Code Injection')	3.32	4	+3 ▲

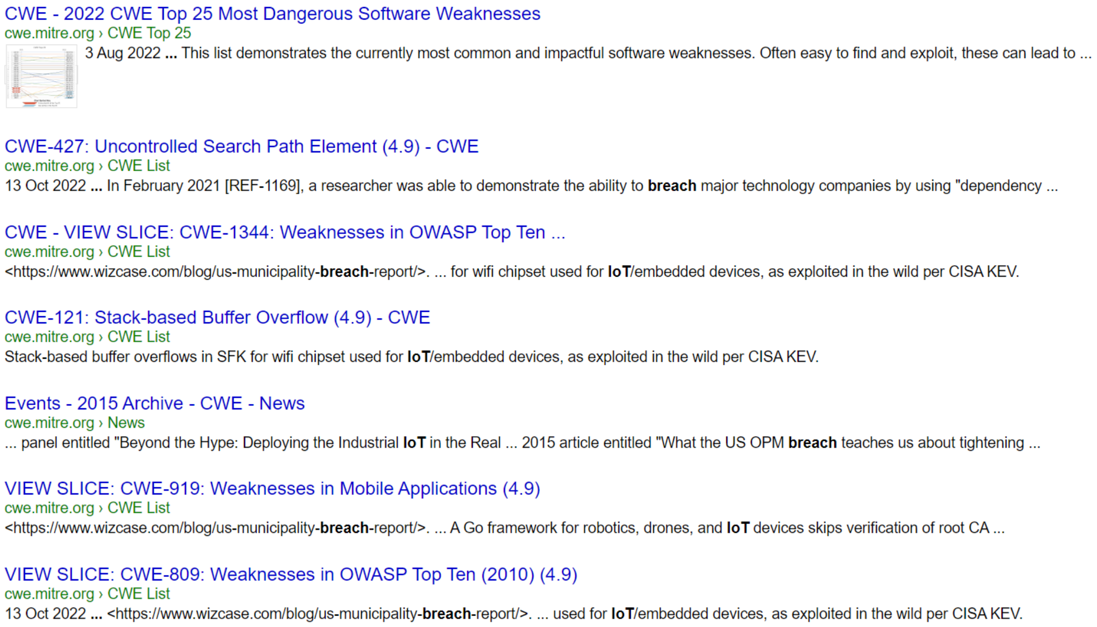
Appendix B: Visual representation of the difference in 2021 and 2022 Top 25 lists

Table. 5[43] Difference for CWE Top 25 in 2021 and 2022.



The screenshot from MITRE explains recent breaches that happened due to H-IOT device Vulnerabilities [44]

Fig. 3. (44) Breaches that happened due to H-IOT device Vulnerabilities.



CWE - 2022 CWE Top 25 Most Dangerous Software Weaknesses
cwe.mitre.org › CWE Top 25
3 Aug 2022 **...** This list demonstrates the currently most common and impactful software weaknesses. Often easy to find and exploit, these can lead to ...

CWE-427: Uncontrolled Search Path Element (4.9) - CWE
cwe.mitre.org › CWE List
13 Oct 2022 **...** In February 2021 [REF-1169], a researcher was able to demonstrate the ability to **breach** major technology companies by using "dependency ...

CWE - VIEW SLICE: CWE-1344: Weaknesses in OWASP Top Ten ...
cwe.mitre.org › CWE List
<https://www.wizcase.com/blog/us-municipality-**breach**-report/>. ... for wifi chipset used for **IoT**/embedded devices, as exploited in the wild per CISA KEV.

CWE-121: Stack-based Buffer Overflow (4.9) - CWE
cwe.mitre.org › CWE List
Stack-based buffer overflows in SFK for wifi chipset used for **IoT**/embedded devices, as exploited in the wild per CISA KEV.

Events - 2015 Archive - CWE - News
cwe.mitre.org › News
... panel entitled "Beyond the Hype: Deploying the Industrial **IoT** in the Real ... 2015 article entitled "What the US OPM **breach** teaches us about tightening ...

VIEW SLICE: CWE-919: Weaknesses in Mobile Applications (4.9)
cwe.mitre.org › CWE List
<https://www.wizcase.com/blog/us-municipality-**breach**-report/>. ... A Go framework for robotics, drones, and **IoT** devices skips verification of root CA ...

VIEW SLICE: CWE-809: Weaknesses in OWASP Top Ten (2010) (4.9)
cwe.mitre.org › CWE List
13 Oct 2022 **...** <https://www.wizcase.com/blog/us-municipality-**breach**-report/>. ... used for **IoT**/embedded devices, as exploited in the wild per CISA KEV.