Cyber Security and Internet of Things

Conference Paper · May 2021

CITATIONS
0

READS
5,283

1 author:

Swapnil Suraj
FNF
1 PUBLICATION **0** CITATIONS

SEE PROFILE

Cyber Security and Internet of Things

25th April, 2021

Swapnil Suraj

Campbellsville University

Table of Contents

Abstract……...iv

List of Figures …….....v

Chapter 1……..1

Introduction……..1

Problem Statement and Purpose of Research……..1

Relevance and Significance…….2

Research Questions……..5

Barriers and Issues……...5

Chapter 2…….....7

Research Literature and Analysis…….....7

Chapter 3…….....14

Methodological Approach Overview…….……14

Methods of Topic Selection and Research Questions Definition…….....14

Methods of Data Collection……...14

Methods of Data Analysis……..15

Methods of Data Reporting…….....15

Chapter 4…….....16

Findings…….....16

Analysis…….....17

Results…….....17

Chapter 5…….....18

Conclusions……....18

Implications…….....19

Recommendations…….....20

References……..21

Abstract

Internet of things and cybersecurity are a rapidly growing phenomenon which cover most new applications of technology in the modern world. This publication seeks to raise awareness for the need of cybersecurity in IoT devices and suggests various methods and models to do so. It also explores reasons behind using certain security methods over others while ensuring and echoing the need to make users aware of the risks and solutions. It also seeks to educate people from industry, academia, and student educators as to why cybersecurity has increased relevance in today's world while at the same time highlighting its use on IoT systems. It seeks to empower users to make decisions based on data and various qualitative methods while imploring them to ponder on the next challenge in this amazing journey of humans.

Keywords: IoT, cyber security, Internet of Things, threats

List of Figures

Figures

Common cyber-attacks for IoT devices and hardware-assisted mitigation techniques…..8

Operation of the data protection system transmitted in the IoT system……10

Conceptual model of cybersecurity assessment for healthcare IoT-based system……12

Chapter 1

Background and Introduction

Introduction

Cybersecurity and the Internet of Things have become even more relevant in modern times. Few decades earlier Cyber Security and the Internet of Things were considered as separate disciplines. They were not studied together. Things have changed drastically over the years and Cybersecurity and Internet of Things have become one of the most studied topics in industry as well as academia.

Cybersecurity primarily revolves around the phenomenon of protecting systems, software and various other computers from attacks on the connected as well as standalone networks. This enables systems to be run securely on any compute environment such as datacenters, personal computers, mobile phones and IoT devices.

Internet of Things is the science of connecting all possible devices with the internet. When a machine or a computer is said to have Internet of Things technology, it implies that the machine can be controlled or monitored by sitting anywhere in the world. It usually has abilities such as monitoring, alarms and recording previously unknown problems to the system.

Problem Statement and Purpose of Research

This paper revolves around the amalgamation of cybersecurity and Internet of Things. Since, including the power of the Internet of Things in any system makes it exponentially more

capable, it becomes important for a scientist or organization to take necessary steps to prevent unauthorized or malicious use. The paper will explore and answer various questions about the implication of using/not using cybersecurity such as what, how and why.

Relevance and Significance

Cybersecurity threats to IoT are especially prevalent in organizations which have extremely powerful Internet of Things ecosystems and tremendous amounts of compute such as self-driving car companies. One such great example of a car company which utilizes Internet of Things systems in its cars is Tesla. They have a host of software and hardware systems integrated in their car which assist and, in some cases, completely take over the control from the driver. If a bad actor were to gain access to their system, it can result in proliferation of multiple years of research to other state sponsored or individual hackers and result in significant monetary loss to Tesla. There might be some bad actors whose intent may be to remotely take control of the car and possibly cause loss of human lives. It becomes extremely important for companies like Tesla to have a strong and dedicated approach to cybersecurity along with the Internet of Things.

The problem has become extremely far ranging in recent times as more Internet of Things devices come online. In today's world people's entire homes are connected to the internet. From the main door deadbolt to the lights in the living room, all are connected to the internet. Any lapses in security have serious impact in modern society. If a person's deadbolt can be compromised remotely then it might cause serious problems for them. It can result in risk of life, injury and in some cases even death. If a hacker is able to remotely compromise someone's security cameras, then they can invade on their privacy. It may result in embarrassment for them,

serious violation of privacy and the hacker may even use this footage to gain intelligence to commit crimes such as theft.

The benefit of solving is multifold. The most important thing is keeping people secure. If organizations and companies can demonstrate that their devices are secure, it increases consumer confidence in those companies. People are more likely to buy from a brand that has a stellar reputation over a brand that may not be as secure. It may also result in other devices in the home being compromised. If a malicious actor is able to gain access to the router/internet gateway in the home, then they may be able to practically access any device. In such cases it becomes even more important to realize the importance of solving cybersecurity issues.

One other example which can be taken is for hospitals. In modern day hospitals most of the equipment is connected to the internet. If a malicious actor is able to gain access to these systems, it may result in catastrophic risk of loss of lives.

There have been multiple attempts across history to solve cybersecurity issues on the Internet of Things. One of the first approaches was to use authentication but with the advent of modern hacking techniques this has become increasingly ineffective and only serves as a first layer of protection.

The second approach has been to employ authentication. This provides significantly elevated levels of protection but comes with its own set of challenges as well. Since Internet of Things devices are sometimes quite small in nature and cannot incorporate the bulky hardware required to process encrypted traffic.

The third approach that has become prevalent more recently has been to use VPNs in protecting and communicating with the IoT devices. This enables less load on hardware and high levels of security. Although, this method has significant inherent challenges as well. It comes

with the risk that if the entire network of the VPN sponsor is compromised, then it may result in all devices on that network to be compromised as well.

The consequences of not solving the problem are far reaching and tremendous in nature. It results in a risk to human lives, capital, and the loss of confidence in the ecosystem of connected devices. All modern machines and factories incorporate some or the other feature of Internet of Things devices. One such example is a steel factory which incorporates sensors to monitor and control the various processes in steelmaking. If a malicious actor is able to compromise the system, then they can jeopardize the steel mill which could result in a huge amount of loss of lives, capital and market reputation. It can have rippling effects across the board. The steel mill might be producing surgical grade steel and hence it may result in non-availability of surgical devices. This could further result in loss of human lives. In the modern world all the supply chains are extremely closely connected, and it is important to recognize their delicate balance.

The goal of the study addresses the research problem because it will answer the fundamental question that causes those issues in the first place. Then the proposed course of study will also delve into some of the current solutions that are being used in the industry. Finally, the study will move towards the ideal future improvements projected for those vulnerabilities.

This research will be highly useful for people from academia as well as the industry. Since it incorporates the current trends in industry it will be invaluable for people working in the industry to use as a reference guide. It also offers general solutions which may be relevant to most industry use cases or serve as a guiding principle for them.

The results have a great potential to be generalized since the paper examines cases which are relevant to everyday uses. It avoids picking topics which are unique and less applicable in general scenarios.

The work incorporated in this paper is completely original. All the thoughts and ideas are the brainchild of the writer. This paper does use external resources, but they are only to support the ideas presented by the author.

Research Questions

This paper would try to answer the 3 big questions - The What, The Why and The How.

1. What are the known and potential cyber security threats in IoT?
2. Why are these cyber security threats so critical?
3. How to improve cyber security for IoT systems?

Barriers and Issues

The problem is significantly difficult to solve because the Internet of Things ecosystem has grown tremendously. It is hard to come up with general solutions that can have a large impact on the entire ecosystem. This pushed the writer to explore ultra-low power consuming, cheap and efficient methods for digressing a viable solution. The paper will require digesting multiple ideas that are out in the industry and then making highly analytical conclusions from them. It also involves the writer to have and develop domain knowledge in this spectrum which demonstrates the ability to learn and digest complex data. There are multiple issues that can occur during the research. One of the first challenges is the obfuscation of good research articles by private organizations which makes it difficult to access industry data. The second challenge

arises in finding solutions that can be applied across a large ecosystem and typically not affected by factors such as geographic region, cost, and skill level.

Chapter 2

Review of the Literature

Research Literature and Analysis

I researched many articles, scholarly papers, journals related to cybersecurity and IoT. Article titled Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics by Yang Lu and Li Da Xu talks about how Internet of Things devices will revolutionize the global ecosystem of interconnected devices. It also illustrates how the development of technologies related to the Internet of Things are still in an infancy stage. It mentions that there are several issues related to this technology that need to be solved. Then it delves deeper into the main issue which is the biggest risk for the Internet of Things which is security. It explores the various ways in which cybersecurity around IoT devices can be used. The key highlights within security that the article explicitly states are the protection and integration of heterogeneous connected devices and technologies which are used in communication with those devices. The primary audience for the article is information security researchers and industry practitioners who would appreciate a broad overview of all the possible challenges and solutions. Even though the article excels at providing the methods of safeguarding IoT system such as RFID authentication, WSN measures and transport layer security enhancements, I felt there were a few things missing and not emphasized enough such as the general characterization of what security means for an IoT device and how it can be applied to consumer grade IoT devices and not just industry. Also, some of the methods proposed in the paper are too specific and require significant changes in the ecosystem such as hardware. A good ideal solution would not necessarily require

specialized resources but rather focus on making the current devices more secure using software on the backend.

Research Paper titled Hardware-Assisted Cybersecurity for IoT Devices by Fahim Rahman, Mohammad Farmani, Mark Tehranipoor and Yier Jin talks about use of hardware in protecting IoT system. The article has a very interesting take on security by assistive hardware which can be embedded in current technologies or can be designed from the group up. The article talks in detail about the potential economic losses and benefits of using a hardware based cyber secure IoT based solution. The article also recognized the challenge of having low power, cost efficient and minimum footprint hardware solutions. One of the things that this article does not completely go over is the challenge of developing the specific hardware and including machine level assembly software to run the required hardware. It would great to explore in more detail about the potential challenges and benefits of creating both hardware and software rather than just overhauling the software. The article talks in detail about the potential pitfalls when dealing with malware. This is especially useful for modern applications such as self-driving cars or camera systems because they are usually affected by malware and need protection.

Figure 1

Common cyber-attacks for IoT devices and hardware-assisted mitigation techniques

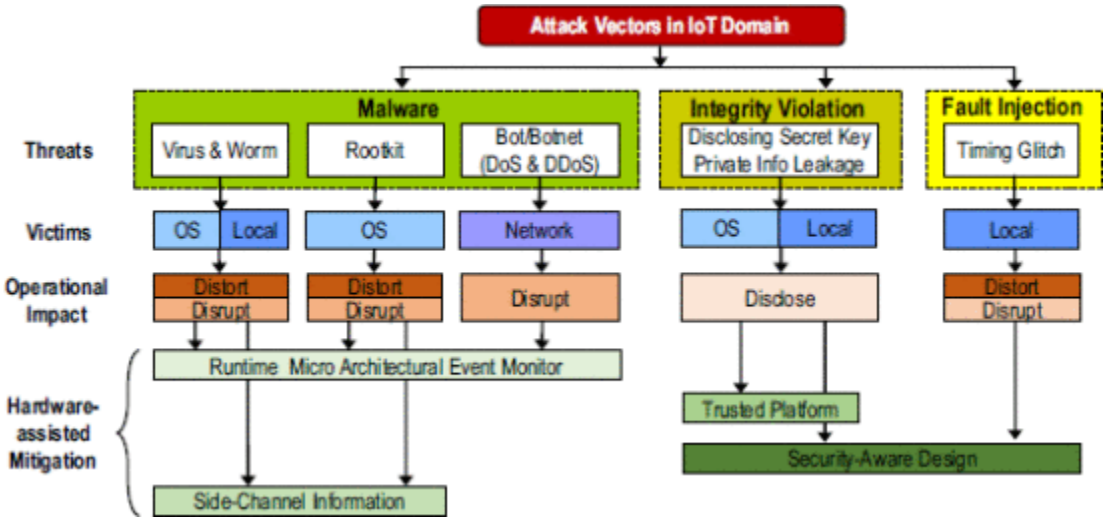

Figure 1 reproduced from the article gives a detailed insight of how IoT threat prevention systems can potentially work. It analyzes the sources of threat, integrity violations and fault injection. The flow chart further describes the use case scenarios that might occur when an attack is taking place. This chart serves as an important function of highlighting the common use cases to the reader which can aid in creating mitigation strategies.

Research article titled Cybersecurity Challenges and Opportunities in the New "Edge Computing + IoT" World by Jianli Pan and Zhicheng Yang talks about the massive shift being witnessed in the adoption of the Internet of Things and the security concerns that arise with those changes. It not only describes the current changes happening in the industry but builds upon the future of IoT and cybersecurity. It describes and delves into everyday application of IoT and their security measures. The everyday uses include smart home automations, transportation, hospitals and health, energy and power grids, robotic assisted devices, and finally industrial scale applications. Further, the article dives deeper into the concepts and fundamentals of building protection in IoT devices. It first analyzes the cybersecurity challenges that exist and then aims to offer potential solutions for it. One of the most interesting points in the article is that it very clearly describes the overall scope of the problem. The current number of IoT devices are in

billions and potentially expected to cross into the trillion-count territory. It becomes vastly important to recognize the size and scale of the development and its potential consequences.

The article also takes a different view at IoT devices from an edge computing perspective. This is immensely useful since most of the consumer as well as industrial grade IoT solutions use a central network to connect to and operate. It also describes the solutions using edge computing devices which usually helps in making the devices smaller, low in energy consumption and usually cheaper. It also enables more software tweaking to manage all the installed devices.

Article titled The cybersecurity in development of IoT embedded technologies by Botir Usmonov, Oleg Evsutin, Andrei Iskhakov, Alexander Shelupanov, Anastasia Iskhakova and Roman Meshcheryakov talks about a specific use case of IoT system which is commonly used called as embedded systems. This means that the IoT technology is embedded in some shape or form into an existing product. Embedded systems are usually stitched together on a hardware level and may share the same resources such as compute, power supply etc. The article dives deep and analyses the challenges and processing of using embedded technologies for IoT systems. It then uses a framework of physical, logical, and virtual components to analyze the level of security that can be achieved. It is fairly technical in nature and addresses the problem on a hardware level. The article has some severe shortcomings because it fails to take practical models or examples but rather focuses on the author's documentation of their own model. This creates several issues which make the practical application of the article less relevant from an industry perspective and makes it purely academic in nature.

Figure 2

Operation of the data protection system transmitted in the IoT system

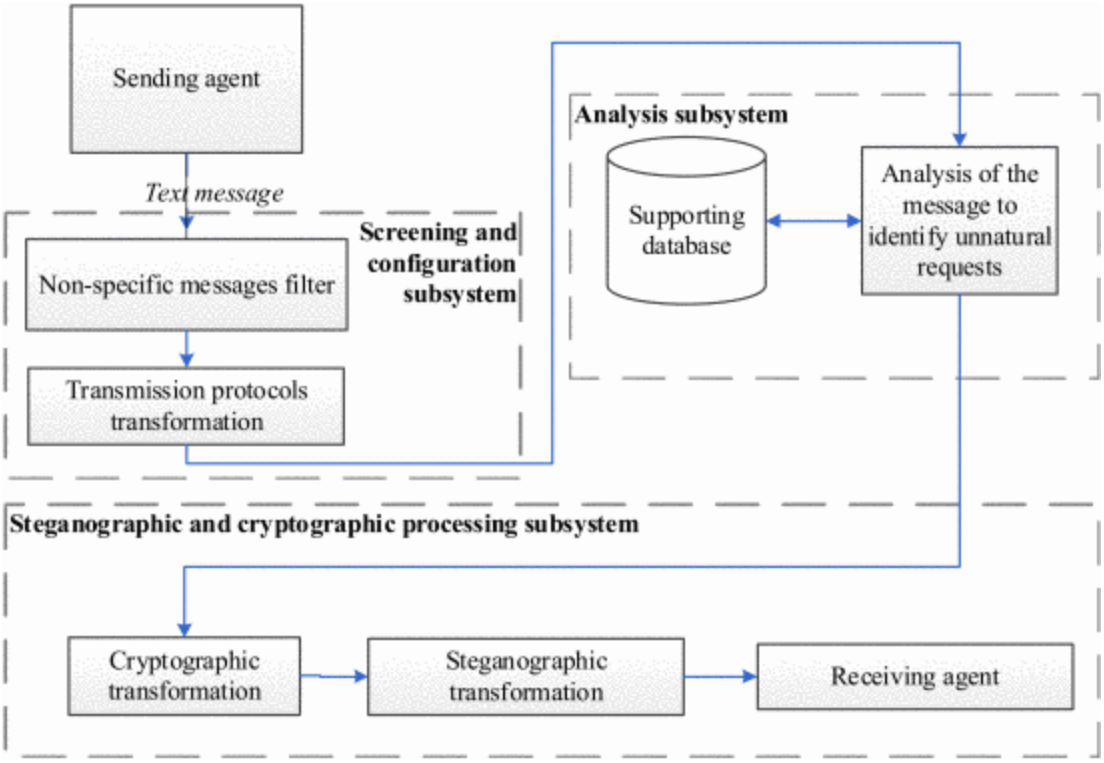

Figure 2 reproduced from the article serves a useful process of identifying a system which works primarily for the protection of data. The system is described as a model and it is difficult to qualitatively or quantitatively analyze the practical application of this model. The article also does not provide any pointers for this.

Article titled Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment by Anastasiia Strielkina, Oleg Illiashenko, Marina Zhydenko, Dmytro Uzun talks about the implications and application of IoT devices in healthcare. It also analyzes the security angle for it. The article takes a comprehensive approach to analyze the scope and scale of increasing IoT devices in healthcare, then changes course to include the complete medical architecture. This is especially the interesting part since it gives a significantly better picture of the overall ecosystem and the ways that it affects complicated medical architecture. It then gives special attention to the analysis of IoT tools using cybersecurity methods, suggests a normative

model for international cybersecurity standards and then uses a case-based technique to analyze a real-world issue.

Figure 3

Conceptual model of cybersecurity assessment for healthcare IoT-based system

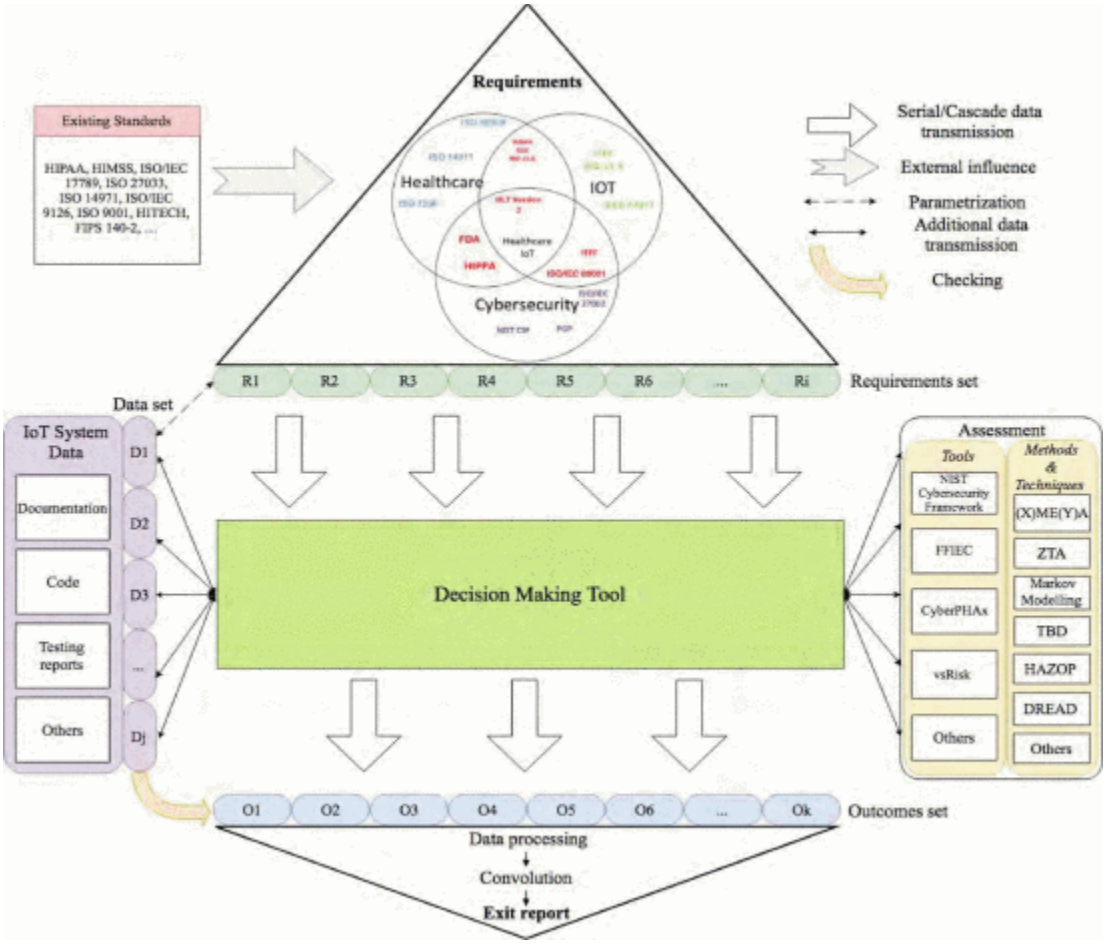

Figure 3 reproduced from the article is especially helpful. It depicts overall ecosystem and workings of an IoT system in healthcare. It serves as a great resource to model and analyze any upcoming challenges that might occur. It also follows a flow pattern which enables the user to think in a specific way and aids in coming up with remedies for cybersecurity threats in IoT.

Paper titled Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks by Katie Boeckl, Danna Gabel, O'Rourke, Michael Fagan, Deloitte & Touche LLP, William Fisher, Naomi Lefkovitz, Katerina N. Megas Karen Scarfone, Ellen Nadeau, Scarfone Cybersecurity, Ben Piccarreta Clifton talks about the growing concerns around privacy and security for IoT devices and services. It highlights the lack of awareness individuals/organizations may have when using IoT devices. The article then highlights some of the security challenges and privacy risks associated with these devices. The concerns around privacy have become more amplified in current times due to several countries and states rolling out their own privacy laws. An organization needs to be compliant with all the existing rules and regulations in the area and this article does a great job of bringing that awareness to these organizations. It then analyzes the differences in security and privacy between traditional IT systems and modern day IoT devices. Further on the article also gives the user great insight in not only managing ongoing and future risks but create a framework which can be replicated across organizations and devices. In my opinion this article is the most comprehensive overview on cybersecurity and IoT, it provides all the requisite points to the user which can help in making decisions and includes a comprehensive list of pitfalls to be aware of.

Analyzing deeper into these resources surfaced many patterns like all the articles focused on first analyzing the security threats to the systems, then some of the articles tried to offer hardware solutions, some of them software and the ones I found least useful provided a model to go on. The model-based approach was least useful since having only a model has its difficulties in applying to real world situations.

Chapter 3

Research Methodology

Methodological Approach Overview

The research methodology used for this paper can be broadly classified into these five steps –

1. Topic Selection and Research Questions Definition
2. Data Collection
3. Data Analysis
4. Data Reporting

Methods of Topic Selection and Research Questions Definition

While selecting the research topic, the criteria that was given highest priority was the relevance, public perception, and the need to increase the awareness around the topic. A brief analysis was done on all the available topics to weigh them on these criteria and finally 'Cyber Security and Internet of Things' was selected as the topic of research. This was also the topic that interested the author the most since it is related to their personal passion in home IoT devices.

Methods of Data Collection

Archival Research was primarily used for data collection for this research which involves accessing manuscripts, documents and records from depositories, libraries, and the internet. For this research, research journals and articles were sourced from digital libraries of reputed

institutes like IEEE (Institute of Electrical and Electronics Engineers) Xplore and ACM (Association for Computing Machinery) to ensure high quality data points, research, and analysis. Keyword search at websites like scholar.google.com and researchgate.net was also completed to get obtain associated resources. Obtaining literature from reputed sources also ensured that authors are well qualified in their field of research and papers are peer reviewed properly. The research papers to be used for reference needed to be very recent (not published before 2017) to ensure updated and relevant data.

Methods of Data Analysis

Content Analysis was primarily used for data analysis for this research which involves study of documents and communication artifacts like texts of various formats, pictures, audio, or video. Content analysis is used here to examine patterns in the written journals sourced from online libraries in a systematic and replicable fashion. After the sources for analysis were selected, few sets of questions and keywords were defined to search through those texts, for example – author's recommendations to improve cybersecurity in IoT, datasets used to support their research, author's views on cybersecurity threats, research methodologies and so on.

Methods of Data Reporting

APA style formatting (6th edition) was used compile and report the data in form of a research paper. The paper follows a systematic approach and divides the content in various sections, easily accessible through table of contents and supplemented with literature references.

Chapter 4

Findings Analysis and Results

Findings

These elaborate the findings based on this article.

1. Large scope of IoT devices- Usually when researchers, academics and people from industry study IoT and security they usually overlook the vast scope of IoT devices. IoT devices by nature are inherently small and its difficult to realize that they are part of the ecosystem. One such example is of cars, if a person buys a new car, they don't think of it as a connect giant computer. But in today's world most cars are basically massive computers which keep sending data back to their brand servers. The cars also have the ability to be controlled, updated and deactivated remotely. Hence, the scope of IoT devices is typically harder to recognize but on a broader view these devices are everywhere.
2. Common issues in implementing security- There are certain constrains which are highly prevalent across IoT devices. These devices are usually very small and manage only small amounts of power consumption, compute and storage. Given the limited nature of the hardware it often becomes difficult to implement some industry standard security software because the system resources are just not enough for the task.
3. Challenges of introducing encryption in security- This risk is related to the previous one and again comes down to limited hardware available. Encryption is typically a compute intensive process that requires the system to have higher resources. With

having a higher compute also comes the challenge of higher power consumption. Since IoT devices are extremely in nature it is difficult to implement these technologies without extensively modifying the hardware.

4. Common ways to increase security in a IoT device- The security of IoT devices can be enhanced in multiple ways. It can be done through encryption, increased awareness of use cases, security protocols and complex models to prevent compromise.

Analysis

This elaborates the analysis that devised based on the findings in the article.

1. Need to increase awareness, security, and encryption standards.
2. Need to make the process of organization that sells IoT devices more transparent and possibly open source.
3. Enhance the availability of IoT devices and knowledge to all people.

Results

This section will describe the aggregated results by the analysis on this paper.

The paper aims to ultimately encourage the use of IoT devices as a force for good. Including the subject of cybersecurity enables to do this because it enhances the level of protection and makes these devices secure and safe for people to use. It also demonstrates the commitment of people in this industry to make this technology accessible for people who traditionally may not be a part of this ecosystem. It seeks to empower through knowledge, security and the right use case for IoT.

Chapter 5

Conclusions, Implications and Recommendations

Conclusions

There are several conclusions that were achieved after the study -

1. The large scope of IoT devices and their security- The IoT industry has become extremely large and involves almost all the new devices/machines and other equipment manufactured. The ecosystem of the devices is becoming more centralized as well as intertwined with other systems. It is not enough to just study some IoT systems in isolation. To analyze the overall scope of the challenge ahead it becomes imperative to analyze using the bigger picture. Hence, while completing a study in this domain a researcher should incorporate the large scope and their definition characteristics for the study.
2. Methods of securing IoT systems such as hardware and software- There are several methods that were discussed in various articles utilized during the course of this study. Some articles leaned towards hardware methods while others leaned towards software methods. Some of the articles had a combination of both. Based on the qualitative analysis run on the methods it was discovered based on real world applications that software methods were easier to implement and required less intervention. Although, some hardware methods are more secure, but they come with their own set of challenges which usually revolve around cost and implementation. Hardware methods are typically well suited for devices that require extremely high levels of security, while software-

based implementations seem to work well for most everyday applications. One of the themes that was common across IoT devices was to keep power consumption low and ensure devices can continue functioning with small compute and limited energy resources.

3. Creating future models to replicate cybersecurity in IoT- This is the future section of the article and involves a unique framework. Since just having a model is rarely useful, it is assumed that the author of the article will provide some methods of practical application of these models. Although, these models offer a certain benefit, which is ensuring that the research and analysis conducted is presented in a manner which is consistent and repeatable.

Implications

This research serves as the pillar for future references on cybersecurity threats and IoT because it gives the reader a general overview of the processes involved in both IoT and cybersecurity. It persuades the reader to understand and explore everyday technologies and the risks that come associated with them. It then gives the reader a direction to explore major challenges and their fixes.

This is useful for both people in academia and industry. People in industry who are working on these cutting-edge technologies and gain from the good practices described and the potential pitfalls while people in academia can benefit from enhancing research on this specific area.

Recommendations

There are several recommendations that can be summarized from the article:

1. Make the process of privacy and security transparent for users: The users of any system have a basic right to understand if their data is secure and how it will be shared. The need of the hour is to make this information transparent and freely accessible to all users. This also helps the user to plan what information and devices they feel comfortable using and sharing their information with.
2. Enable opens source access in ecosystems: This is the first step in bringing transparency to connected ecosystems and ensuring their safety. Open-source technologies are usually vetted by a group of people and significantly harder to compromise. The change of any bug slipping through is significantly reduced. Having an open-source code also gives the users a huge boost in confidence since they know what exactly they will be sharing and how that data will be used. Creating an open ecosystem also encourages individuals and organizations to build on top of the current systems to enhance capabilities and deliver an excellent product.
3. Bring awareness about the scope and impact of IoT: It is important to spread awareness about the true scope of the IoT and ensure that it is used for the good of humanity.

I can summarize that IoT is a force for good and using it in an ethical, safe and responsible manner will shape the future of humanity.

References

Boeckl, K., Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K. N., ... & Scarfone, K. (2019). *Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks*. US Department of Commerce, National Institute of Standards and Technology.

Rahman, F., Farmani, M., Tehranipoor, M., & Jin, Y. (2017, December). Hardware-assisted cybersecurity for iot devices. In *2017 18th International Workshop on Microprocessor and SOC Test and Verification (MTV)* (pp. 51-56). IEEE.

Lu, Y., & Da Xu, L. (2018). Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103-2115.

Pan, J., & Yang, Z. (2018, March). Cybersecurity Challenges and Opportunities in the New" Edge Computing+ IoT" World. In *Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization* (pp. 29-32).

Strielkina, A., Illiashenko, O., Zhydenko, M., & Uzun, D. (2018, May). Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment. In *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 67-73). IEEE.

Usmonov, B., Evsutin, O., Iskhakov, A., Shelupanov, A., Iskhakova, A., & Meshcheryakov, R. (2017, November). The cybersecurity in development of IoT embedded technologies. In *2017 International Conference on Information Science and Communications Technologies (ICISCT)* (pp. 1-4). IEEE.