Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 6 (2023)

Role of Cyber Security in Mitigating Challenges, Threats and to Enhance Prevention Methods in the Modern Digital Era.

Dr. V. Shobana[1] Dr. A. Nirmala[2]

1 Associate Professor, Department of Computer Science with Cyber Security, Dr. N. G.P. Arts and Science College, Coimbatore.

2 Professor, Department of Computer Science with Cognitive Systems, Dr. N. G.P. Arts and Science College, Coimbatore.

Abstract

Due to the development of technology and its increased usage it is necessary to protect the data from various Cyber Attacks. Cyber Security plays a vital role to enhance the efficiency of technology by providing security by protecting the data from the attackers. The focus of this research is on the various issues of cyber security because of new technologies. It also looks at the newest ways to protect against cyber-attacks and the changes happening in cyber security. These attacks can cause serious harm to businesses and their customers. The majority of businesses have adopted digital technology in response to the COVID-19 pandemic. By relying on digital systems, a company can easily be a predator for cyber-criminals.

Keywords: Cyber Security, Threats, risk and digital era

I.Introduction

The way things are turned into digital files has made it possible to store all kinds of information, including private data. Security is about keeping digital information safe from being stolen or damaged [1]. It's important to make sure the information is kept private and can still be accessed when needed. But as technology advances, cybercrimes are also increasing, becoming more numerous and harder to understand. Many factors contribute to the surge in cyber-crime, including the use of inferior software, obsolete security tools, and flaws in design and programming. Many individuals are unaware of how to safeguard themselves against the abundance of hacking tools readily accessible on the internet. And cyber-criminals can make a lot of money from it. To find weaknesses in a computer system and then attack it, hackers create stronger tools to use. New types of attacks are happening that are hard to find. The internet is becoming more important in our daily lives.

As online business process like shopping and banking, a lot of data is being collected. This has led to the creation of better ways to keep our information safe. Cybercrime keeps changing, which makes it hard to deal with and avoid new threats. Securing the internet is really hard because there are lots of tricky threats out there [2]. It is essential that we comprehend various techniques and popular subjects in information security in order to keep our systems safe. The use of innovative techniques can lead to an increase in cyber-attacks on the internet. Cybercriminals often update their malware.

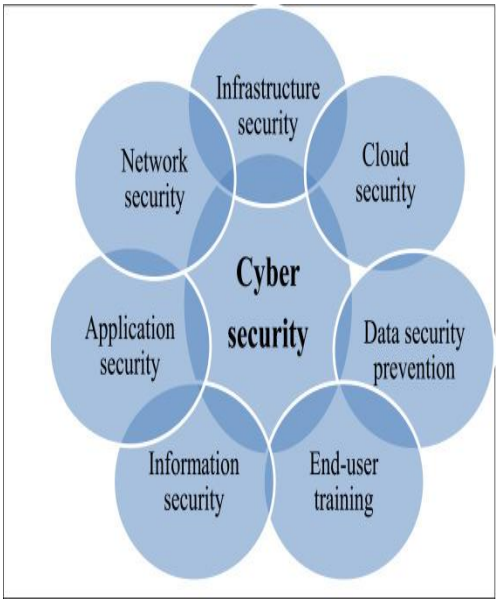

Figure 1: Different Types of Security

To use new technical flaws. In certain instances, they seek out novel technological capabilities in order to pinpoint vulnerabilities in malware. With the help of new internet technology and a large online population, cyber criminals can easily target and impact numerous individuals [3]. Protecting computer systems has become increasingly difficult for organizations with the advancement of new cyber techniques and the frequency of attacks. They also need to find new ways to gather information. It is important for us to make an effort to decrease cybercrime in order to ensure a safe and secure online future. The future is dedicated to researching reliable internet and effective systems. In the future, it is increasingly crucial to develop methods for monitoring individuals' identities and advertisement factors [4]. This study centres on personal data as the main focus in various forms of cybersecurity issues. Businesses around the world are spending a lot of money to address cybersecurity issues, which are increasing every year. However, overcoming this challenge can seem complicated as attackers continuously look for new vulnerabilities in people, organizations and technology.

II.Literature Review

Yuchong Li et.al illustrate about many private companies and government institutions worldwide are currently grappling with the challenge of cyber attacks and the potential dangers of wireless communication technology [5]. Today's world depends heavily on electronic technology and protecting this data from cyber attacks is a challenge. The goal of cyber attacks is to cause financial harm to businesses. In other cases, cyberattacks may have military or political goals. Some of the harm includes PC viruses, data breaches, Data Distribution Services (DDS), and other methods of attack. To achieve this goal, different organizations use various solutions to prevent damage caused by cyber attacks. Cybersecurity tracks real-time information about the latest computer data. Till date, many different methods have been proposed by researchers around the world to prevent cyber attacks or minimize the damage they cause. Some methods are in the operational phase and others are in the research phase.

Vidya L. Badadare et.al describe about requirements of cyber security and their digital era [6]. The purpose of this study is to comprehensively review the standard advances presented in the field of cybersecurity and study the challenges, weaknesses and strengths of the proposed approaches. Different types of new top-down attacks will be discussed in detail. Standard security frameworks are discussed along with the history and methods of first generation cybersecurity. Additionally, emerging trends and recent developments in cybersecurity as well as security threats and challenges are presented. The comprehensive review study presented to IT and cybersecurity researchers is expected to be useful. Smartphones have expanded the playing field for hackers to infiltrate and disrupt the digital realm. In the field of social networks, people are allowed to share thoughts, feelings, and life

status without any restrictions, which leads to a situation of handshake for hackers. If cybersecurity policies are properly implemented, they will neutralize cyber threats.

Mohit Jain et.al discuss about paper examines research on cybersecurity, which includes different types of cybersecurity [7]. The aim of this research is to comprehend the vulnerabilities, dangers, and deficiencies of electronic systems, encompassing both physical and virtual components, as well as internal networks. Cybercrime can happen anywhere and at any time, and the effects can be very serious. It is not limited to just one area. Cyber Security encompasses a blend of innovative technologies, protocols, and strategies. Cyber security aims to keep applications, networks, computers, and important information safe from attacks. In computing, security includes keeping the network safe and protecting physical resources. The hacker steals or damages computer programs or information just to cause trouble or confuse the people they trick. Currently, people think digital protection is important for any technology to work well.

Esra Altulaihan et.al illustrate about the cyber security threats and their future directions. The aim of this research is to comprehend the vulnerabilities, dangers, and deficiencies of electronic systems, encompassing both physical and virtual components, as well as internal networks. Cybercrime can happen anywhere and at any time, and the effects can be very serious were it is not limited to one area. Cyber Security encompasses a blend of innovative technologies, protocols, and strategies. Cyber security aims to keep applications, networks, computers, and important information safe from attacks. In computing, security includes keeping the network safe and protecting physical resources. In the current situation, the organization's activities are not safe, so some security goals have been developed to stop harmful actions. The article talks about dangers and ways to stop them, and a look at what threats may come in the future in online security.

Xiang Liu et.al illustrate about cyber security challenges faced in e-commerce sector. The technology has really helped businesses to do things in a better way. It changed the old ways of doing business and made them better. New technologies change the way products and services are made and how much they cost for businesses. Business is when people trade things with each other. Their business involves selling products or services for a monetary exchange. E-commerce or e-business refers to the use of electronic technology for conducting business activities. In online shopping, everything is done using the internet. Three important things in e-commerce are online shopping, selling things on the internet and bidding in online auctions. Researchers from different fields are working to make it even more useful and profitable. However, these changes have also caused some problems for the industry. One big problem for e-commerce is keeping it safe from hackers and other online threats.

III.Methodology

The research methodology used for managing cyber security risk by IoT Security system. The existing system and proposed system were discussed to manage challenges faced with preventive measures.

Existing Methods

The Internet of Things (IoT) technology has given us many new opportunities, but it has also made our connected systems more at risk for attacks that could cause problems with keeping information private, making sure it's accurate, and making sure the systems are working when they should. Creating a safe environment for IoT devices is a big challenge. It needs a methodical approach to find and fix security problems. Thinking about cybersecurity research is very important [8]. It helps us figure out how to make things safe from online threats. This helps us deal with new risks that come up. To make IoT safe, experts need to create strict security rules. These rules will be the basis for making devices, chips, and networks safe. Creating these specifications needs people from different areas, like cybersecurity experts, network planners, system designers, and domain experts to work together. The biggest problem in IoT security is making sure the system can protect against both attacks that it already know about and ones it don't know about yet. So far, the IoT research community has found some important security problems with the way IoT systems are built. These worries include problems with staying connected, communicating, and managing systems. This research paper gives a clear and complete review of the current issues and security ideas connected to the Internet of Things. It study common security problems with the way IoT devices are set up, like how they connect, communicate, and are managed. It start the basis of IoT security

by looking at the latest ways that people are attacking it, the dangers, and the newest ways to keep it safe. Also, it create security targets to measure if a solution meets the needs of specific IoT uses.

Proposed Methodology

This study wants to find out how safe data is when it's sent online. This research used a method called descriptive qualitative approach, which means it looked at existing literature. This study shows that it's safe to use the internet and can help avoid dangerous things [9]. This study will warn people to be careful when using the internet. Stealing someone's identity can lead to data theft, and it is a very serious problem. As a result of data theft, people are being made to create a new password. The harder it is to prove something's identity, the more valuable it is and the more likely it is to be stolen. It will also take time to create the documents again.

It need to make sure that our important computer systems are safe from hackers and other threats. This is really important for the safety and economy of every country. Keeping internet users safe has become very important when creating new technologies and government rules. Because only using technology cannot stop crime, it's important for the police to investigate and prosecute cybercrime. Many countries and governments are implementing stringent regulations on cyber security in order to avoid data breaches.

Effective measures play a crucial role in safeguarding public services as businesses and organizations undergo digital transformation. According to changes it need to be considered as they are a top priority for countries and companies undergoing digital transformation. The summary emphasizes the value of implementing uncomplicated programs and approaches to build reliable cybersecurity governance, without the risk of hacking or data tampering, as part of digital transformation [10]. According to the study, even as companies adopt more technology across all industries, including banking, they increase flexibility and sales opportunities, while reducing costs incurred internally. The retraining time for employees, who may not be familiar with or lack the necessary skills at this time due to the rapid changes taking place globally.

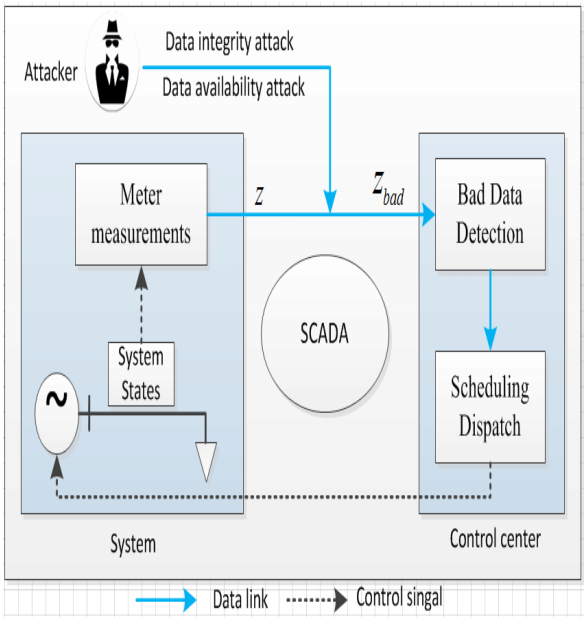

Figure 2: Methodology diagram for cyber security system [11]

The employees need to be more involved in these projects if it want them to have an impact on the company's performance level. Therefore, activities should not only focus on supporting business resilience to the risks associated with cyber security threats but also improve the level of staff needed for the task is more complex as businesses automate processes through the adoption of technology. Opportunity to simultaneously reduce costs incurred internally such as employee retraining time. Furthermore, it was emphasized that implementing Secure Development Plans can help reduce the potential hazards of embracing new technology.

IV.Results

Effective measures plays a crucial role in safeguarding public services as businesses and organizations undergo digital transformation [12]. According to changes it need to be considered as they are a top priority for countries and companies undergoing digital transformation. The summary emphasizes the value of implementing uncomplicated programs and approaches to build reliable cybersecurity governance, without the risk of hacking or data tampering, as part of digital transformation.

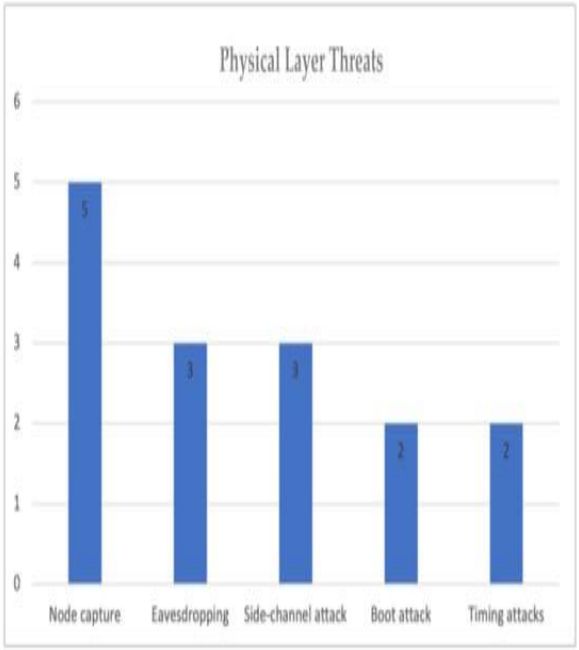

Figure 3: Graphical result of System analysis [8]

According to the study, even as companies adopt more technology across all industries, including banking, they increase flexibility and sales opportunities, while reducing costs incurred internally. Department, such as retraining time for employees, who may not be familiar with or lack the necessary skills at this time due to the rapid changes taking place globally, employees need to be more involved in these projects if we want them to have an impact on the company's performance level [11]. Therefore, activities should not only focus on supporting business resilience to the risks associated with cyber security threats but also improve the level of staff needed. As technology keeps getting better and new online dangers keep appearing, there may still be weak points in even really good security. So, it's really important for companies going through digital transformation to predict future technology and plan for cyber security to keep improving their ways of doing things. Taking action to improve security can reduce the chances of problems in the future when using technology.

This means making sure employees have training and programs to recognize and react to cyber threats. Businesses using new technology like IoT devices [13], 5G networks, or quantum computing need to do careful risk assessments before using them. This is very important. Organizations that want to be as safe as possible need to keep checking how well their cybersecurity plans, preparations, deployments, and monitoring are working.

V.Conclusion And Future Work

At the most basic level, organizations have important cybersecurity activities in place, like planning, preparing, deploying, and watching for security threats. But they don't have an overall plan for cybersecurity. The processes are not fully developed and people are working on their own to improve security. It doesn’t have any information on how well these security methods are working. At the ground level it has planned for our system, organizations should have a clear plan for keeping their computer systems safe. This plan should outline how they get ready for potential cyber attacks, how they put in place security measures, and how they keep an eye on their systems for

any threats. In the surveillance phase, it needs to regularly check for weaknesses in our systems by doing penetration tests or vulnerability scans.

VI.References

[1] Antonio, "Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey," https://www.mdpi.com/2079-9292/12/8/1920, pp. 1-13, 2023.

[2] Ana, "Australia's Cyber Security," https://www.taylorfrancis.com/chapters/edit/10.4324/9780429399718-34/australia-cyber-security-ana-stuparu, pp. 1-14, 2021.

[3] Diptiben, "Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review," https://www.authorea.com/doi/full/10.22541/au.166385207.73483369, pp. 1-12, 2021.

[4] Eunkyung, "The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence," https://link.springer.com/article/10.1007/s10796-019-09977-z, pp. 367-363, 2021.

[5] Y. Li, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," https://www.sciencedirect.com/science/article/pii/S2352484721007289#d1e368, pp. 8176-8186, 2021.

[6] Vidhya, "Cyber Security Need of Digital Era: A Review," https://www.researchgate.net/publication/343988551_Cyber_Security_Need_of_Digital_Era_A_Review, pp. 9-12, 2018.

[7] Mohit, "Cyber security: Current threats, challenges, and prevention methods," https://ieeexplore.ieee.org/document/10009154, pp. 1-12, 2021.

[8] Fredick, "Research communities in cyber security vulnerability assessments: A comprehensive literature review," https://www.sciencedirect.com/science/article/pii/S1574013723000187?via%3Dihub, pp. 1-28, 2023.

[9] George, "Chasing damages for mass data breaches: Devastating hacks reveal gaping flaws in Australia's cyber laws," https://search.informit.org/doi/abs/10.3316/informit.104612779860976, pp. 14-18, 2023.

[10] A. Georgiadu, "A Cyber-Security Culture Framework for Assessing Organization Readiness," https://www.tandfonline.com/doi/abs/10.1080/08874417.2020.1845583, pp. 452-462, 2022.

[11] Khairur, "Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework," https://www.sciencedirect.com/science/article/pii/S1110866522000226, pp. 383-402, 2021.

[12] Kelsey, "Metaphor identification in cybersecurity texts: a lightweight linguistic approach," https://link.springer.com/article/10.1007/s42452-022-04939-8, pp. 1-15, 2022.

[13] Yahya, "Agile Approaches for Cybersecurity Systems, IoT and Intelligent Transportation," https://ieeexplore.ieee.org/document/9656744?denied=, pp. 1-6, 2021.