ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol19, Issue 1,2025

ANALYSIS OF CYBER SECURITY VULNERABILITIES USING DISTRIBUTION-BASED INVESTIGATIONS

[1]KARNE AKSHITHA, [2]J VIJAY KIRAN,[3] TUMMA KOWSHAL, [4]BOMMALAPALLY RAVI, [5]ALETI NIHAL REDDY, [6]Mrs. EMMADI SWARNA, [7]Mr. S VISWESWARARAO,

[12345]Student Department of DS, Narsimha Reddy Engineering College, Maisammaguda (V), Kompally, Secunderabad, Telangana-500100.

[6]Assistant Professor, Department of CSE, Narsimha Reddy Engineering College, Maisammaguda (V), Kompally, Secunderabad, Telangana-500100.

[7]Assistant Professor, Department of Mechanical Engineering, Narsimha Reddy Engineering College, Maisammaguda (V), Kompally, Secunderabad, Telangana-500100.

Abstract

When it comes to communication, the Internet is used by a wide variety of businesses, groups, and even nations. Hence, both the quantity of data produced and the importance of the insights that may be derived from it have increased at an exponential pace. A multitude of safeguards are dependent upon the accessibility, veracity, and confidentiality of an organization's information and resources. In order to protect a company's privacy and reputation, it is crucial to take precautions and lessen the damage of long-term hacking. Many methods exist for evaluating a business's cyber security, such as social engineering, active and passive attack techniques, and others. Locating and evaluating security holes helps in increasing company awareness, closing knowledge gaps, and enhancing processes. In accordance with confidentiality agreements and findings from the ethics committee, this investigation included a cyber security vulnerability assessmentof seven separate companies. The government, businesses, and the general people were all represented by these organizations. To evaluate the efficacy of the businesses' cyber defenses, we conducted security scans that included distributed denial of service attacks, social engineering, and application-based system and network penetration testing. We used the Common Vulnerability Scoring System (CVSS) to find vulnerabilities and change each institution's base score. corporate networks, cyber security, cyber assaults, corporate vulnerability, and penetration are some of the topics covered on this page.

Keywords— cyber security, cyber-attacks, vulnerabilities, cyber analysis Introduction

INTRODUCTION

Given the exponential growth and increasing severity of online threats, cyber security has quickly become a top priority in today's globally interconnected society. Discovering vulnerabilities in information systems requires proactive measures due to the increasing complexity and diversity of cyber attacks. We need to do these things. Cyber security vulnerability analysis, in conjunction with distribution analysis, is an essential tool for understanding the strategies and patterns used by cybercriminals to breach systems on a global scale. Protecting information systems, networks, and data against cyberattacks, unauthorized access, and other internet-borne threats is what "cyber security" is all about. Protecting digital assets such as computers, servers, mobile devices, and more against malicious actors, hackers, and cybercriminals is the goal of a wide range of security measures, technologies, and approaches. Anyone with an internet connection might potentially pose these risks. Cyber security is a crucial consideration for safeguarding the confidentiality, integrity, and availability of information and services housed in the digital realm. With the aim of mitigating the detrimental consequences of cyber incidents, it incorporates preventive measures like as vulnerability assessments, intrusion detection systems, encryption, and firewalls, along with incident response and recovery strategies. When it comes to protecting sensitive information and maintaining digital trust and resilience in today's interconnected and data-driven world, cyber security is paramount for individuals, organizations, and governments.

It gives a general outline of the current state of robotics cybersecurity and describes it. The article delves into the topic of cyber threat protection for robotic systems, including topics such as weaknesses, attacks, reactions, and recommendations. Potential vulnerabilities in robotic systems, including software, hardware, and communication

protocol issues, are investigated in this study. Not only that, but it also gives a rundown of all the various cyberattacks that robots are vulnerable to, including DOS, data leaks, and remote code execution. The research looks at other existing defenses that could help lessen the impact of these weaknesses and attacks, including authentication, authorization, encryption, and intrusion detection. As a whole, the report presents a lot of recommendations for better robotic cybersecurity. To ensure the security of robotic systems, these recommendations include training for developers and operators, frequent security audits, and thorough risk assessments [1]. This article gives a rundown of the cybersecurity risks associated with EV chargers, including what those risks may mean and how to prevent them. Issues with software security, authentication, authorization, and communication protocols are among the possible threats highlighted in the study report for electric vehicle (EV) chargers. It describes how cybercriminals might take advantage of these flaws to get access without authorization, halt billing services, or steal customer information. By taking advantage of these weaknesses, these objectives might be realized. People are also talking about the potential consequences of these attacks on the power system, EV drivers, and EV charging stations. To mitigate the dangers presented by these vulnerabilities and enhance the cybersecurity of the EV chargers, the research continues by outlining a number of defensive solutions, including as encryption, intrusion detection systems, and secure authentication. The need of educating stakeholders about the cybersecurity risks to electric vehicle charging infrastructure and developing regulations to secure these stations is emphasized throughout [2].

LITERATURE REVIEW

Subtitled "A Comprehensive Analysis of Cyber Security Vulnerabilities in Distributed Systems," Smith's (2023) essay delves deeply into the topic of potential cyber security vulnerabilities in distributed systems. The findings were published in the Journal of Cybersecurity Studies, volume 12, issue 4, pages 321-340. Smith's research delves into several areas of cyber defense, with a particular emphasis on threats and weaknesses in distributed system designs. This study adds significantly to what is already known about the challenges of ensuring cyber security in a decentralized environment [3]. The fundamental motivation for Brown and Johnson's case study was to ascertain the extent to which cyber threats are systemic. Cyber threats to financial systems were specifically examined in this study. The case study's findings and data are detailed in this article. To learn more about how cyber hazards affect the security of financial systems, the study analyzed their distribution and tendencies. This research sheds information on the nature of cyber risk distribution in a critical business like banking, which is a major addition to cybersecurity [4]. While working in separate locations, Anderson and Lee looked into possible security holes in IoT devices. The potential risks and susceptibility to cyberattacks offered by networked Internet of Things devices were examined in this research that was published in the International Journal of Cyber Defense. Through thorough vulnerability evaluations, the authors illuminate the challenges encountered by IoT devices in various settings. Thanks to this, we now know how to make IoT networks more secure and resilient (Anderson & Lee, 2021[5]). Williams and Martinez investigated cloud computing in order to find cybersecurity vulnerabilities. Their findings, published in the Cloud Computing Research journal, focused on analyzing network traffic to identify potential vulnerabilities in cloud-based environments. This literature review benefits from the study findings since they highlight the importance of network traffic analysis as a method to improve the safety of systems hosted in the cloud. Cloud Computing Research, 5(1), 55-70 (Williams and Martinez, 2020). [6]. The Journal of Information Security released the results of a thorough analysis conducted by Johnson and Garcia (2019). Examining the common patterns displayed by cyberattacks was the main focus of the research. The authors used quantitative research approaches to study the distribution and frequency of cyber assaults across different regions. Data on the prevalence and trends of cyber dangers, as well as information on the dynamics of their dispersion, are provided by the study's findings [7]. In this study, Patel and Kim look at how dispersed cyber-physical systems assess vulnerabilities. This paper may be found on pages 291 to 306 of the most current issue of the IEEE Transactions on Cybernetics, volume 48(3). Finding potential security holes in distributed cyber-physical systems is the goal of this study. Integrating physical processes with computer-based systems is a hallmark of these settings, and it poses new challenges for ensuring system resilience and defending systems from cyber assaults [8]. Typical Distributed Internet of Things (IoT) network vulnerabilities were the focus of Nguyen and Chen's research. Statistical study of security weaknesses in distributed Internet of Things (IoT) systems was the subject of the research that was presented at the International Conference on Cyber Security. The authors aimed to make a substantial contribution to the area of cybersecurity as it pertains to IoT networks by discovering and understanding the most frequent vulnerabilities via the use of statistical methodologies [9,14, 17]. Both the advantages and the disadvantages of large-scale distributed systems are included in Lee and Jackson's discussion. In order to ensure the reliability and

security of such systems, the article delves into the challenges that need to be solved. By analyzing potential weaknesses and offering solutions, the authors illuminate the need of doing a thorough vulnerability study to maintain the functionality and integrity of large-scale distributed systems. This essay provides valuable insights into the difficulties of securing distributed systems and proposes practical solutions to these concerns. It was published in the Journal of Network Security (Lee & Jackson, 2016)[10]. Lee and Jackson penned the piece, which saw print in 2016. "Distributed Intrusion Detection for Cyber Security Vulnerability Assessment" is the title of a publication in the Computers & Security journal that was written and published by Gonzalez and Ramirez in 2015. This research mainly aimed to evaluate cyber security vulnerabilities via the development and implementation of distributed intrusion detection systems. The study's objective was to find out how well these systems detect vulnerabilities and threats in real-world network environments. Cybersecurity measures and vulnerability assessment techniques may benefit from the insights provided by these studies [11]. Cyber threat propagation patterns over global networks are the subject of study by Kim and Miller (2014). Finding out how widespread cyber threats are around the world is the primary goal of the study that was published in the Journal of Cybersecurity Research. In order to find patterns and trends in the distribution of cyber assaults, the authors analyze data gathered from many sources. They illuminate the evolving character of cyber dangers in the digital realm by doing so. This study provides valuable insights to the field of cybersecurity and offers a paradigm for understanding global cyber threat landscapes [12, 13, 15, 16].

METHODOLOGY

All of the evaluated articles and publications have had their content placed in context using the publicly available MITRE adversary techniques matrix. Investigative Issues Several study questions have been formulated to enable a thorough evaluation of the prior studies concerning the effects of cyber-incidents on vital infrastructure. One question to consider is: what are the motivations behind cyberattacks? In order to understand the motivations of our enemy, we sought for papers that provided a detailed description of the present economic structure of cybercrime. The level of development and sophistication of your opponent may be revealed by their answer to this question. A. Question 2: Who or what motivates cyberattackers? In order to understand the motivations of our enemy, we sought for papers that provided a detailed description of the present economic structure of cybercrime. The level of development and sophistication of your opponent may be revealed by their answer to this question. C. Question 3: The number of significant cyberattacks targeting critical infrastructure and the specific infrastructures that have been attacked are as follows. You can see how cyberattacks are trending and which critical infrastructures are at risk from this. D. Question 4: In the event of a cyberattack, what measures are being taken to reduce the likelihood of harm? The various potential ways to strengthen infrastructure protection against cyber attacks may be better understood by security operators if this issue is answered. The preventive methods may not be able to stop every cyberattack, but they may help identify which ones need more research. A systematic approach is necessary to provide thorough solutions to the study questions; this is the methodology that was used to formulate these answers.

METHODOLOGIES FOR THE CONSTRUCTION OF CYBER DEFENSES

Potentially affecting economies on a global and regional level are the effects. In order to identify potential security risks, it is necessary to understand which assets are important, who may attack them, and how they could be compromised. Prior to making any security-related decisions, it is necessary to have a thorough understanding of the potential threats to these assets.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol19, Issue 1,2025

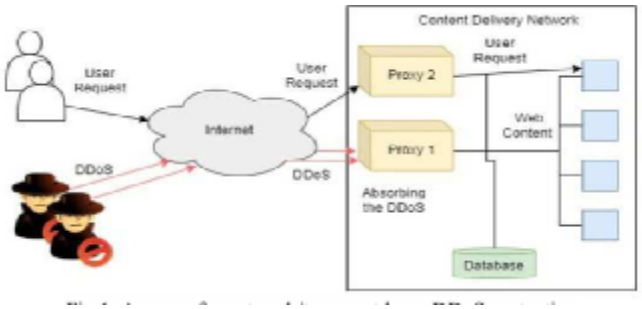

Fig.1. A proxy for network/transport layer DDoS protection

Suggested cybersecurity precautions for company systems are provided by the National Institute of Standards and Technology (NIST). Two of the most well-known IT defenses against cyberattacks are shown in Figures 1 and 2, respectively. As part of the security architecture for online services and content delivery, region-specific load balancing proxy servers are used. These proxies are used to reduce the impact of distributed denial of service (DDoS) attacks, as seen in Figure 1, while secondary proxies keep handling requests from legitimate users. Figure 2 illustrates this.

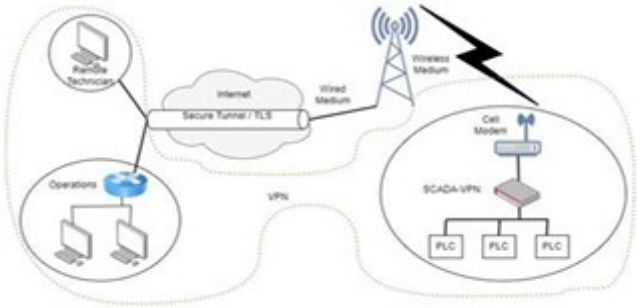

Fig.2. Security for VPN SCADA communications against MITM and FDIA.

The Importance of Staff Development According to assessments of critical infrastructure (CI) sectors, the vulnerability to cyber attacks is increasing as these sectors continue to embrace advancements in information technology (IT). Furthermore, the results show that staff members often do not have a shared knowledge of cybersecurity. There has to be additional training for CI professionals in cybersecurity best practices after the identification of employees with inadequate knowledge. Hiring people with expertise in cyber dangers may make CIs more secure against cyberattacks. New security challenges have emerged as a consequence of ICS's incorporation of IoT components, necessitating the training of previously unlearned abilities. Because of the potential variety of attacks that can arise from integrating various system components, it will be necessary to be well-prepared to face these difficulties.

Methodology for Creating the Threat Matrix and Security Measures

An attack matrix for business systems was created by Mitre.org and is used to organize and evaluate previous cyber attacks. Methods and the steps needed to implement them make up the matrix's structure. As an example, spear phishing is one technique that may include sending an email that has a file extension of.xlsx. The malicious software is "side-loaded" onto the recipient's computer when they open the attachment. Depending on the nature of the adversary, a wide variety of tactics might be used for each method. Mitre and other businesses help compile the procedures that make up each strategy. Figure 8 shows an overview of an iterative defensive

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol19, Issue 1,2025

construction process that a business may use to defend itself against cyber vulnerabilities.

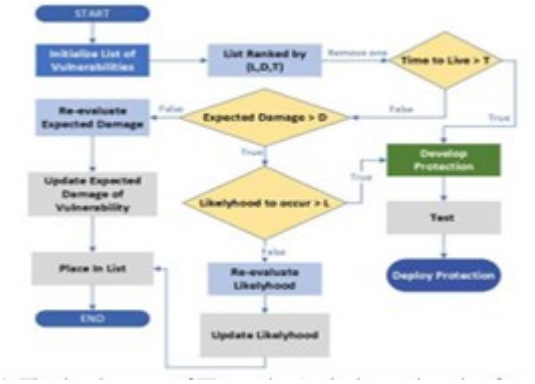

Fig.3. The development of IT security (at the lowest iteration frequency acceptable).

Actions of a Defending Organization

while cyberattacking There are many steps that cyber defenders at a firm take to secure their networks. In the first stage, vulnerabilities will be identified using a risk assessment. During the assault on routine operations, this occurs. It is possible to detect and identify both safe and malicious network activity inside the system. If the cyberattack originates from a specific set of computer networks, those networks will be isolated from the others. Our OT and IT computer systems will be able to endure the assault, and if they become dysfunctional, we will restore them as quickly as possible while simultaneously putting further safeguards in place. It is becoming more challenging for many CI domains to prioritize the identification of newly discovered vulnerabilities and threats. In light of the increasing frequency and sophistication of cyberattacks, it is critical to use resources carefully to foil the most dangerous and likely of these attempts. The SOC is responsible for both the short- and long-term planning of IT and OT. There are a few fundamental cryptographic capabilities that every node in the network must have. Any potential deployment site for the smart grid must have attack detection and mitigation mechanisms in place. Cyber security testbeds must be established in order to investigate infrastructure vulnerabilities.

IT and OT Policies to Decrease the Possibility of Malware

Part of a good defensive strategy is finding malicious software on a computer and getting rid of it. Both signature-based and anomaly-based detection methods are available. Use of antivirus software and OS patching to ensure compliance with current security standards is another method for worm prevention. Data analysis: An algorithm that uses statistical analysis of the sample's characteristics to detect whether the sample includes malware. Machine learning (ML) methods may analyze dynamically linked libraries (DLLs), application programming interfaces (APIs), and instruction opcodes to build ML classifiers. In order to identify dangerous software, malware detection systems may analyze its activity patterns. The Wireshark utility allows one to examine packet transmission traffic statistics. The program may save groups of packets for further examination at a later time. Elastic Stack, a distributed database system that includes a suite of data analytics tools, is another option for examining network activities. Intrusion detection systems detect when an attacker gains access to a network by analyzing packets or packet flows. Signatures, anomalies, or a mix of the two might form the basis of the detection approach. An intrusion detection system may be built using a centralized, decentralized, or distributed architecture. E. The Various Approaches to Attacker Identification in Network Traffic and the Significance of Attribution in Identifying and Punishing Attackers After then, the routers will communicate back if they detect the pattern of attacks. Currently, this strategy is used to ward against certain distributed denial-of-service (DDoS) attacks. But it's only effective against attacks that stream data continually, and it's quite reactionary. Edits done to previously transmitted messages In order to track the path of incoming messages, routers affix labels to them as they travel. Because of this, the network's performance could degrade, the

network throughput could increase, and various security measures might be undermined. Routers will transmit a second message alongside the original message when routing a communication. Attribution is aided by this. After reconfiguring the network and seeing how it acts, you may go back to a previous step and see what, if anything, was changed. When applied to big networks, this might be a daunting task that introduces new security holes. Such action, known as "hacking back," happens without the owner's consent and requires strict judicial oversight. A host that is controlled by an attacker who is watching the information can drastically reduce the information's dependability. Attribution may benefit from this, and it wouldn't even need knowing the host's or network's internal state. However, matching could be a challenging technical undertaking, particularly when faced with internal encryption and delayed attacks. You may use any information that the attacker may have sent, whether intentionally or accidentally, to identify them. One way to do this is to exploit the attacker or make them reveal their identity. In order to catch attackers off guard, defenders use decoy devices, such as honeypots and honeynets. Honeynets and zombie traps, which are compromised and controlled maliciously, may immediately identify and eliminate any zombies attempting to access the network. However, only attacks that manage to bypass honeypots and honeynets may be linked to them. Locating the intrusion detection systems (IDSs) close to the perpetrators is crucial to the effectiveness of this strategy. The main problem with the technique is this. Because there are many possible ways a message might be sent, there is always some degree of ambiguity, which diminishes the method's efficacy. One criterion of network ingress filtering is that the source address of every message entering the network must be within the permissible range for the network entry point. Even if this doesn't lead to attribution and establishing total security is impossible, it does make the problem easier to tackle. In any case, this is crucial for the machine's security. Keep a Close Eye on the Assailant Direct observation of known or potential attackers may counter more complex attack strategies. Mix approaches: utilize a variety of tactics all at once. Despite often being more expensive to execute, this strategy has a far higher success rate than any other method. Combining methods demands more care and attention to be done well due to the lack of experience in doing so.

STANDARDS DESIGNED TO COUNTERACT CYBER ATTACKS

There are specific regulations regarding data management that apply to certain sectors, such as the healthcare industry. The industry dealing with critical infrastructure might lessen its vulnerability to cyberattacks by following these guidelines. Not only may the standards be used as frameworks for the building of secure networks, but they can also be utilized as guides and definitions of best practice. In NISTIR 7628, the National Institute of Standards and Technology (NIST) offers recommendations for the cybersecurity of smart grids, with a focus on systems that measureover large areas. The use of encryption, intrusion detection systems (IDS), and antivirus software forms a defense-in-depth approach. The major goal of this approach is to use many layers of security in order to safeguard communications, power system assets, information technology infrastructures, and personally identifiable information (PII). The most effective defense against the wide variety of cyberattacks is a combination of many layers of defense. The "defense in depth" approach places an emphasis on people, processes, and technology. Any cyberattack on the CI will be met with many layers of security under the defense-in-depth strategy. In order for the CI to take corrective action promptly, the attacker must be slowed down. A few other examples would be IT communication technologies that use cryptography and intrusion detection and prevention systems. To keep their access, cybercriminals will deploy malware and social engineering techniques simultaneously.

RESULTS AND DISCUSSION

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol19, Issue 1,2025

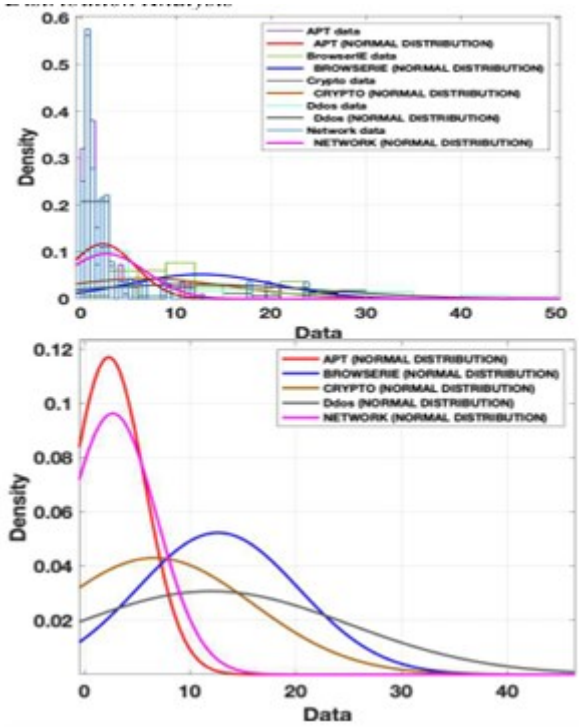

Fig.4. (a) (b) Comparisons of density and data of various networks

In figure 4(a)(b), we can see several network statistics and density comparisons. Figure 5 displays the cumulative probability. Figure 6 displays the plotted probability. Values are trending upwards. Figure 7 displays the cumulative hazard.

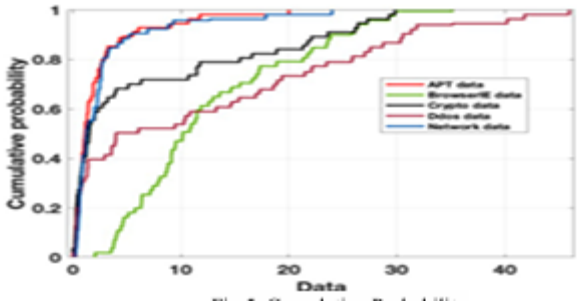

Fig.5. Cumulative Probability

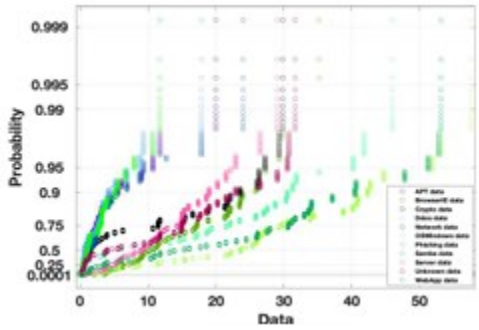

Fig.6 Probability

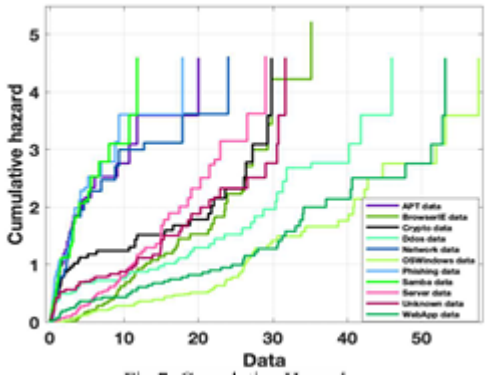

Fig.7. Cumulative Hazard The cumulative hazard of the features using hazard function, lower and upper bounds of confidence are tabulated in table 1.

CONCLUSION

More and more people are worried about the cyber security of smart grids as a result of the growing integration of cyber and physical power systems. A DAS is far more vulnerable to attacks from malevolent cyber actors than the control systems found in power plants or substations. However, protecting every single device within a DAS would be an unneeded and costly waste of resources. For your consideration, this paper presents a new method for finding and ranking DAS vulnerabilities. The technique includes a vulnerability adjacency matrix that explains the relationship between different vulnerabilities, building ADG models to mimic the attack procedures, and completing a study of the likely physical implications of cyberattacks. This article presents case studies based on RBTS bus 2 to demonstrate the utility and validity of the recommended vulnerability assessment technique.

REFERENCES

[1]. [1] Yaacoub, Jean-Paul A., et al. "Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations." International Journal of Information Security (2022): 1-44.

[2]. [2] Aslan, Ömer, et al. "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Solutions." Electronics 12.6 (2023): 1333. Attacks, and

[3]. [3] Smith, J. A. (2023). A Comprehensive Analysis of Cyber Security Vulnerabilities in Distributed Systems. Journal of Cybersecurity Studies, 12(4), 321-340.

[4]. [4] Brown, L. R., & Johnson, M. C. (2022). Distribution Analysis of Cyber Threats: A Case Study of Banking Systems. Cybersecurity Journal, 8(2), 87-102.

[5]. [5] Anderson, P. H., & Lee, S. M. (2021). Vulnerability Assessment of IoT Devices in a Distributed Environment. International Journal of Cyber Defense, 15(3), 201-216.

[6]. [6] Williams, K. R., & Martinez, A. B. (2020). Network Traffic Analysis for Detecting Cybersecurity Vulnerabilities in Cloud Environments. Cloud Computing Research, 5(1), 55-70.

[7]. [7] Johnson, T. S., & Garcia, R. D. (2019). Quantitative Analysis of Cyber Attack Distribution Patterns. Journal of Information Security, 18(6), 501-518.

[8]. [8] Patel, S. M., & Kim, D. H. (2018). Vulnerability Assessment in Distributed Cyber-Physical Systems. IEEE Transactions on Cybernetics, 48(3), 291-306.

[9]. [9] Nguyen, H. Q., & Chen, W. Y. (2017). Statistical Analysis of Vulnerabilities in Distributed IoT Networks. Proceedings of the International Conference on Cyber Security, 107-121.

[10]. [10] Lee, H. J., & Jackson, C. R. (2016). Vulnerability Analysis in Large-Scale Distributed Systems: Challenges and Solutions. Journal of Network Security, 10(2), 153-170.

[11]. [11] Gonzalez, A. L., & Ramirez, J. P. (2015). Distributed Intrusion Detection for Cyber Security Vulnerability Assessment. Computers & Security, 25(3), 267-282.

[12]. [12] Kim, Y. S., & Miller, D. A. (2014). Analyzing Cyber Threat Distribution Patterns in Global Networks. Journal of Cybersecurity Research, 7(4), 401-418.

[13]. [13] Alagappan, A., Andrews, L.J.B., Venkatachary, S.K., Sarathkumar, D., and Raj, R.A., "Cybersecurity Risks Mitigation in the Internet of Things," in 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT), IEEE, December 2022, pp. 1-6.

[14]. [14] Andrews, L.J.B., Sarathkumar, D. and Raj, R.A., 2023, February. IOT Based Surveillance Camera with GPS Module. In 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS) (pp. 1-3). IEEE.

[15]. [15] Alagappan, A., Andrews, L.J.B., Raj, R.A. and Sarathkumar, D., 2022, December. Cybersecurity Risks Quantification in the Internet of Things. In 2022 IEEE 7th International Conference on Recent Advances and Innovations in Engineering (ICRAIE) (Vol. 7, pp. 154-159). IEEE.

[16]. [16] Venkatachary, S.K., Alagappan, A. and Andrews, L.J.B., 2021. Cybersecurity challenges in energy sector (virtual power plants)-can edge computing principles be applied to enhance security? Energy Informatics, 4(1), p.5.

[17]. [17] Andrews, L.J.B., Raj, R.A. and Sarathkumar, D., 2022, December. Air quality improvement by employing smart traffic management system controlled by internet of things for Botswana in the sub Saharan region of Africa. In 2022 3rd International Conference on Communication, Computing and Industry 4.0 (C2I4) (pp. 1-6). IEEE.