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.ijsem.org
Vol 19, Issue.1 March 2025

USING DISTRIBUTION ANALYSIS TO PROBE CYBER SECURITY VULNERABILITIES

K.S.N.Neeharika [1], G.Lakshmikanth [2],
PG Scholar [1], Dept of CSE, Sree Rama Engineering College, Tirupati – 517507.
Assistant Professor [2], Dept of CSE, Sree Rama Engineering College, Tirupati – 517507

***Abstract*—In many different settings, companies, groups, and even governments utilize online communication as a means of involvement. This has led to an explosion in both the amount of data generated and the value of insights drawn from it. Information and assets belonging to a business must be protected in a multi-layered manner to guarantee its availability, authenticity, and secrecy. Taking preventative actions and limiting the impact of permanent hacks are of the utmost importance in safeguarding a company's privacy and image. To find out where a company's cyber defenses are lacking, hackers may use social engineering tests, active and passive attack strategies, and more. In order to increase corporate knowledge, close gaps, and improve procedures, it is necessary to first identify and then prioritize vulnerabilities. Seven different businesses were subjected to a cyber security vulnerability assessment as part of this inquiry, which adhered to confidentiality agreements and ethics committee reports.**

The public sector, private industry, and civil society were all represented by these groups. Port, online, application-based system, and network penetration tests, as well as distributed denial of service assaults and social engineering, were used to assess the efficacy of the companies' cyber security infrastructures. Each institution's base score was adjusted and flaws were identified using the Common Vulnerability Scoring System (CVSS). This article contains many keywords related to enterprise networks, cyber security, cyber attacks, penetration, and vulnerability.

Cyber risks, cyber-attacks, cyber-analysis, and keywords Hey there!

1. INTRODUCTION

Due to the increasing number of online threats, cyber security has become a major problem in today's globally interconnected society. The increasing sophistication and diversity of cyberattacks need preventative measures to identify security holes in data infrastructure. 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 intrusion, cyberattacks, and other internet-based threats is what "cyber security" is all about. It includes a wide range of measures, tools, and techniques developed to protect digital assets against threats posed by malicious actors, hackers, and cybercriminals. Anyone with an internet connection might potentially pose these risks. Cybersecurity is a crucial consideration for safeguarding the confidentiality, integrity, and availability of information and services housed in the digital realm. The purpose is to lessen the impact of cyber incidents by the use of preventive processes such as vulnerability assessments, intrusion detection, encryption, firewalls, incident response plans, and recovery plans. In today's interconnected and data-driven world, cyber security is crucial for individuals, organizations, and governments to protect sensitive data and maintain digital trust and resilience. Provides a high-level description of the current state of robotics cybersecurity.

It takes a look at cyber attacks, weaknesses, countermeasures, and recommendations as they pertain to safeguarding robotic systems. This study investigates potential robotic system vulnerabilities, including issues with hardware, software, as well as transmission protocols, are investigated. 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. In order to help prevent these vulnerabilities and attacks, the research explores additional existing countermeasures such authentication, authorization, encryption, and intrusion detection. The report concludes with several recommendations for enhancing robotic cybersecurity. Among these recommendations is the need of frequent security

ISSN:2454-9940
www.ijsem.org
Vol 19, Issue.1 March 2025

audits, thorough risk assessments, and developer and operator training to ensure the security of robotic systems [1].

The article summarizes the cybersecurity vulnerabilities associated with EV chargers, their potential consequences, and the solutions that have been suggested to counteract 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 steal sensitive information, halt billing services, or gain illegal access. These objectives might be accomplished by taking advantage of these weaknesses. Potential consequences for electric car owners, charging infrastructure, and the electrical grid are also being considered in relation to these types of attacks. The paper continues by outlining several defensive strategies that might be used to enhance the cybersecurity of EV chargers and mitigate the dangers associated with these vulnerabilities. These approaches include secure authentication, intrusion detection systems, and encryption. It stresses the need of legislation, regulations, and best practices for securing electric vehicle chargers and raising stakeholder knowledge of the cybersecurity risks to this infrastructure [2].

II. LITERATURE REVIEW

In his 2023 paper "A Comprehensive Analysis of Cyber Security Vulnerabilities in Distributed Systems," Smith thoroughly investigates potential cyber security vulnerabilities in distributed systems. Pages 321-340 of the Journal of Cybersecurity Studies, volume 12, issue 4, include the study presentation.

Among the many aspects of cyber security that Smith explores in his research are the risks and vulnerabilities associated with distributed system designs. The challenges of ensuring cyber security in a decentralized environment are better understood because to this study [3].

The major goal of the case study that Brown and Johnson conducted was to ascertain the extent to which cyber risks are prevalent. Cyber risks to financial systems were specifically examined in this study. This article presents the case study's facts and findings. In order to have a better grasp of how cyber hazards impact the security of financial systems, the study examined their patterns and distribution. By shedding knowledge on the nature of cyber risk distribution in a crucial business like banking, this work contributes significantly to the field of cybersecurity [4].
In a decentralized environment, Anderson and Lee looked at possible security holes in IoT enabled devices.
The potential risks and susceptibility to cyberattacks of networked Internet of Things devices were examined in this research that was published in the International Journal of Cyber Defense. The authors conducted thorough vulnerability evaluations to illuminate the challenges encountered by Internet of Things devices in various settings. For the purpose of making IoT networks more secure and resilient, this information was helpful (Anderson & Lee, 2021[5]).

Williams and Martinez investigated cloud computing in order to find cybersecurity vulnerabilities. Cloud Computing Research presented their study, which aimed to analyze network traffic in order to find potential vulnerabilities in cloud-based environments. The study findings illuminate the significance of network traffic analysis as a method to enhance the safety of cloud-based systems, which contributes valuable information to this literature review. Cloud computing research, volume 5, issue 1, pages 55–70, (Williams and Martinez, 2020). [6].

An in-depth analysis was conducted by Johnson and Garcia (2019) and was later published in the Journal of Information Security. The major focus of the research was to analyze the typical trends shown by cyberattacks. Cyber assault frequency and regional distribution were studied by the authors utilizing quantitative research approaches. Findings from the study shed light on the patterns and frequency of cyber threats as well as their distribution dynamics [7].

The assessment of vulnerabilities inside distributed cyber-physical systems is the subject of Patel and Kim's study. The most current issue of the IEEE Transactions on Cybernetics, Volume 48(3), pages 291–306, has the paper. Finding potential security holes in distributed cyber-physical systems is the goal of this study. There are additional challenges in ensuring system resilience and defending them from cyber assaults in these contexts due to the integration of computer-based systems with physical processes [8].

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN:2454-9940
www.ijsem.org
Vol 19, Issue.1 March 2025

Typical vulnerabilities of Distributed Internet of Things (IoT) networks were the focus of this research by Nguyen and Chen. 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].

Lee and Jackson go over the ins and outs of large-scale distributed systems, including their vulnerabilities. This article delves into the challenges that need to be met to ensure the reliability and security of these kinds of technologies. In order to keep large-scale distributed systems running smoothly and securely, the authors highlight the need of vulnerability analysis by examining potential weaknesses and offering solutions. 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). The number ten. Published in 2016, the piece was written by Lee and Jackson.

Computers & Security released a paper by Gonzalez and Ramirez (2015) called "Distributed Intrusion Detection for Cyber Security Vulnerability Assessment.". The research mainly focused on developing and implementing distributed intrusion detection systems to evaluate cyber security vulnerabilities. Examining how well these systems discover vulnerabilities and potential threats in network environments was the driving force behind this study. Cyber security measures and vulnerability assessment techniques may be improved with the use of the insights provided by these outcomes [11].

Cyber threat trends in global network propagation are the subject of study by Kim and Miller (2014). The goal of the study, published in the Journal of Cybersecurity Research, is to better understand the global scope and distribution of cyber threats. Cyber assault distribution trends and patterns are uncovered by the authors' study of data acquired from various sources. They illuminated the evolving character of cyber dangers in the digital realm by doing so. Insightful findings for the field of cybersecurity and a framework for understanding global cyber threat landscapes are provided by this study's findings [12, 13, 15, 16].

III. METHODOLOGY

The data presented in the articles under consideration has been placed in perspective by way of the MITRE group's publicly available adversarial techniques matrix.

Investigative Issues

Our goal in formulating these research questions is to delve deeply into the existing literature on the effects of cyber-incidents on critical infrastructure.

First Question: What are the objectives of cyberattackers? We sought for materials that provided a detailed description of the present economic structure of cybercrime in order to understand the motivations of our enemy. The opponent's level of complexity and developmental stage may be inferred from their answer to this question.
Question 2 (B): What are the motivations for cyberattacks? We sought for materials that provided a detailed description of the present economic structure of cybercrime in order to understand the motivations of our enemy. The opponent's level of complexity and developmental stage may be inferred from their answer to this question.
Thirdly, how many major cyberattacks have attacked critical infrastructure, and which specific facilities have been the targets of these attacks? You can see how cyberattacks are evolving and what critical infrastructures are at risk from this. D. Question 4: What measures are being taken to reduce the likelihood of cyberattacks and their potential consequences? If this question can be answered, security operators will be able to learn about the many methods for bolstering infrastructure defenses against cyberattacks. Preventative methods may not be able to stop every cyberattack, but they may help identify which ones need further research. A systematic approach is necessary to provide thorough solutions to the research questions; this methodology was used to formulate the answers to these questions.

IV. METHODOLOGIES FOR THE CONSTRUCTION OF CYBER DEFENSES

Potentially affecting economies on a global and regional level are the effects. To find out what kinds of security risks exist, we look at the assets that are valued, the people who would want to attack them, and the ways those assets may be compromised. The basis for making security decisions is understanding

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN:2454-9940
www.ijsem.org
Vol 19, Issue.1 March 2025

the potential damage that may be inflicted on these assets.

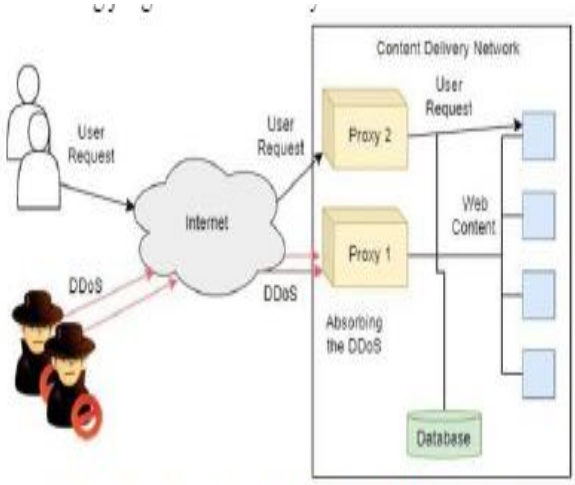


Fig.1. A proxy for network/transport layer DDoS protection

Recommendations for cybersecurity safeguards for company systems are provided by the National Institute of Standards and Technology (NIST). Two well-known IT solutions that may ward against hackers' assaults on networks are shown in Figures 1 and 2. As part of the security architecture for online services and content distribution, region-specific load-balancing proxy servers are used. The purpose of these proxies is to reduce the impact of distributed denial of service (DDoS) attacks, as seen in Figure 1, while secondary proxies keep real customers' demands met. Figure 2 illustrates this.

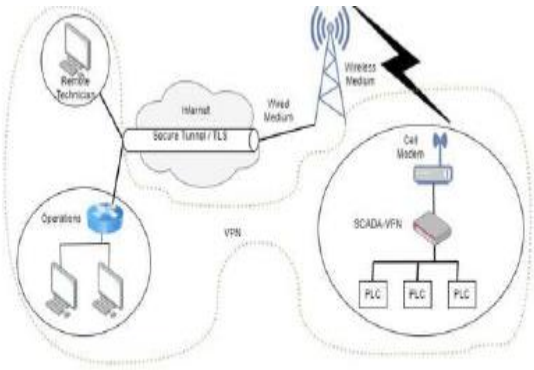


Fig.2. Security for VPN SCADA communications against MITM and FDIA.

A. Reason to Train Personnel

Researchers have shown that critical infrastructure (CI) sectors are becoming more vulnerable to cyber attacks as they adopt new IT innovations. The results also show that staff members often don't have the same grasp of cybersecurity concepts. More training in best practices for cybersecurity should be provided to CI personnel in light of the identification of employees with insufficient knowledge. Hiring people with expertise in cyber dangers may make CIs more secure against cyberattacks. Problems with security have arisen as a consequence of ICS's incorporation of IoT components, necessitating the training of new personnel to address these issues. Overcoming these obstacles will need being ready for a variety of attacks that might arise from combining various parts of the system.

B. Process for the Development of the Threat Matrix and Protections

The work of Mitre.org has led to the development of an attack matrix for business systems, which has been used for the purpose of cataloguing and analyzing past cyberattacks. The procedures and the processes that need to be followed to carry them out are organized in the matrix. An example of this would be spear phishing, which involves sending an email with an attachment that ends in.xlsx. The attachment will side-load malware onto the recipient's PC the moment they open it. 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. As seen in Figure 8, an overview of the methodology, an organization's strategy for securing its cyber vulnerabilities may include an iterative defensive construction process.

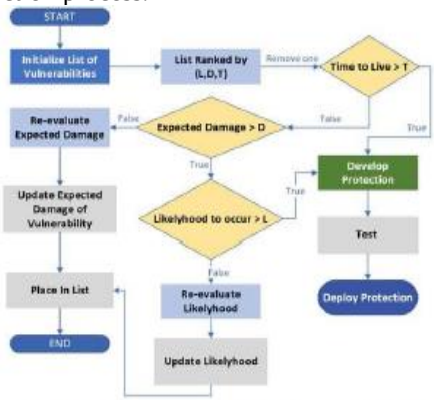


Fig.3. The development of IT security (at the lowest iteration frequency acceptable).

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN:2454-9940
www.ijsem.org
Vol 19, Issue.1 March 2025

C. Actions of a Defending Organization during a Cyber Attack

Cyber defenders at an organization use a multi-step process to safeguard their networks.
In the first stage, vulnerabilities will be identified using a risk assessment. This takes place when normal activities are under assault. It is possible to detect and identify both safe and malicious network activity inside the system. If it is found that any computer networks were the source of the cyber attack, those networks will be isolated from the rest of the network. We are prepared to weather the storm, and if it does knock down our operational technology (OT) and information technology (IT) computer systems, we will restore them as quickly as possible while simultaneously putting in place extra safeguards.
These days, it's hard for many CI domains to tell whether newly discovered vulnerabilities and threats pose the most risk. Cyberattacks are becoming more common and sophisticated, so it's important to use resources properly to protect against the most dangerous and likely ones. The SOC is responsible for both the short-term and long-term planning of the IT and OT departments' futures. Every node in the network has to have some basic cryptography capabilities.
Any potential deployment site for the smart grid must have attack detection and mitigation mechanisms installed. In order to study infrastructure vulnerabilities, cybersecurity testbeds must be established.

D. IT and OT Procedures to Reduce the Risk of Malware

Two parts of a good defensive strategy are finding computer virus and removing it. Two main methods exist for detection: one that relies on signatures and another that uses anomalies. Another way to avoid worms is to use antivirus software and update operating systems to match the latest security criteria. Data analysis: An algorithm that uses statistical analysis of the sample's attributes 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. When looking at dangerous software, malware detection algorithms may spot patterns in its activity.
The Wireshark utility allows one to examine packet transmission traffic statistics. You may save whole packet collections for further examination with this handy tool. 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. A detection method could rely on signs alone, on anomalies alone, or on a hybrid of the two. Intrusion detection systems may be designed using a centralized, decentralized, or distributed architecture.

E. Attribution's Role in Spotting and Punishing Attackers, as Well as the Various Methods for Doing So in Attack Network Traffic

Next, the routers will communicate back whenever they detect the pattern of attacks. Currently, this strategy is used to ward against certain distributed denial-of-service (DDoS) attacks. However, it is only effective against attacks that continually stream data and is very reactionary.
Edits made to previously delivered messages In order to track the path of incoming messages, routers affix labels to them as they go. This could lead to a decline in the network's performance, the increased bandwidth and potential vulnerabilities in various authentication methods.
Routers will transmit a second message along with the original message when they route a communication. This is useful for assigning credit.
Set the network up again while keeping an eye on how it's acting, and then go back to the beginning with a better idea of what changed (if anything). When applied to big networks, this might be a daunting task that introduces new security holes.
The owner's consent is necessary for this action, which is called "hacking back," and it requires strict legal oversight. The data's credibility can take a major hit if it comes from a server that an attacker is using to keep tabs on it.
Without knowing the host's or network's internal state, this can be useful for attribution. When dealing with internal encryption and delayed attacks, matching becomes a technologically challenging operation.
Whether intentionally or accidentally, the attacker's transmissions may be used to identify them. You may do this by taking advantage of their vulnerabilities or by making them reveal their identity.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN:2454-9940
www.ijsem.org
Vol 19, Issue.1 March 2025

Defenders use decoy devices, such as honeypots and honeynets, to draw attackers into their traps. Instantaneously exposing any zombies attempting to access the network is possible using both honeynets and zombie traps, which are infiltrated and maliciously operated devices.

Contrarily, honeypots and honeynets can only record attacks that manage to bypass them.

Ideally, the intrusion detection systems (IDSs) would be placed close to the intruders, as their placement determines the method's success rate.

This is the main problem with the approach. Since a message might go any of many possible routes, there is always some degree of ambiguity, which diminishes the method's efficacy. Due to the nature of network entrance filtering, all incoming messages must adhere to the specified range for the network entry point's approved source addresses. Despite the fact that this does not lead to attribution and that total security is impossible to achieve, it only simplifies the problem.

However, this is absolutely necessary to guarantee the machine's safety.

Keep an eye on the assailant directly. By keeping tabs on known or potential attackers, it is feasible to foil their more complex tactics.

Mix approaches: utilize a variety of tactics all at once. Despite often being more expensive to execute, this strategy has a considerably higher success rate than any other method.

Combining approaches demands more care and attention to be executed correctly due to the lack of experience in doing so.

V. STANDARDS DESIGNED TO COUNTERACT CYBER ATTACKS

Data management regulations are industry-specific; for example, those pertaining to the management of medical records. Sectors dealing with critical infrastructure might lessen their vulnerability to cyberattacks by following these guidelines. In addition to providing frameworks for the creation of safe networks, the standards may be consulted for definitions of best practices and as guidance for their implementation. The standard NISTIR 7628 provides guidelines for smart grid cybersecurity, particularly as it relates to wide-area measurement systems.

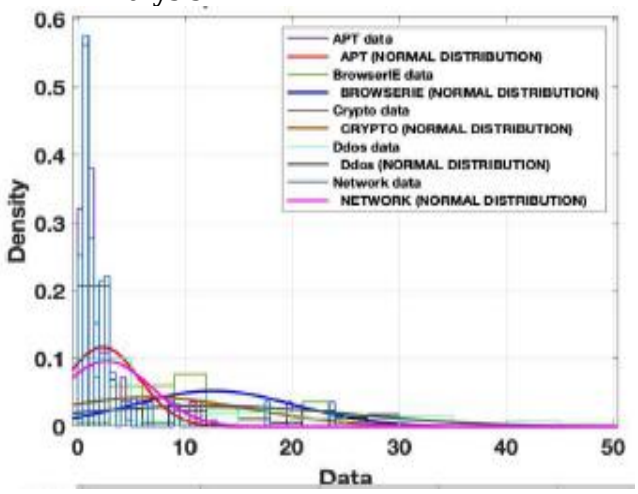
A. NIST Recommendations for the Cybersecurity of Smart Grids

The use of encryption, intrusion detection systems (IDS), and antivirus software forms a defense-in-depth approach. Information technology infrastructures, communications, power system assets, and personally identifiable information (PII) are the main targets of this strategy's multi-layered defenses.

The best strategy to defend against the different types of cyberattacks is to combine many layers of security. The "defense in depth" approach places an emphasis on people, processes, and technology. In order to protect the CI against cyberattacks, the defense-in-depth strategy employs many layers of security. In order for the CI to take corrective action promptly, the attacker must be slowed down. Intrusion prevention systems and other IT communication technologies that use encryption are more examples. In order to keep their access, cybercriminals will deploy social engineering with malware.

VI. RESULTS AND DISCUSSION

A. Threats Firewall – Vulnerability Analysis using Distribution Analysis



INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN:2454-9940
www.ijsem.org
Vol 19, Issue.1 March 2025

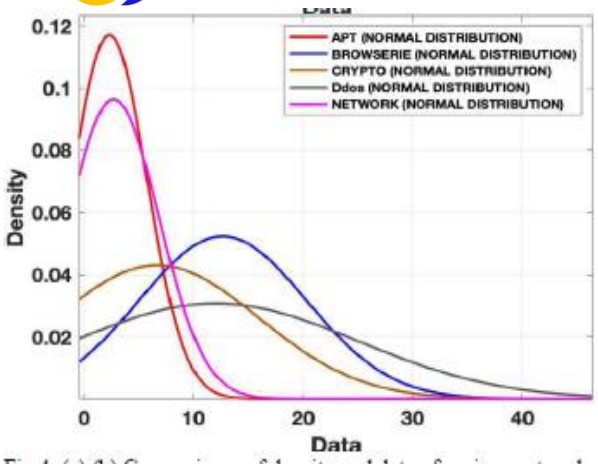


Fig.4. (a) (b) Comparisons of density and data of various networks

Figure 4(a) shows the results of comparing the data and density of different networks (b). In figure 5, we can see the total likelihood. Figure 6 shows a visualization of the probability. You can see that the values are going up. Figure 7 displays the cumulative hazard.

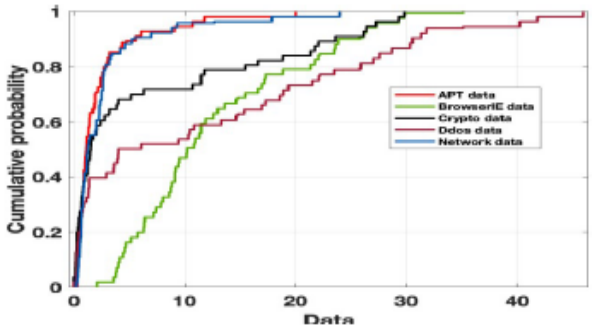


Fig.5. Cumulative Probability

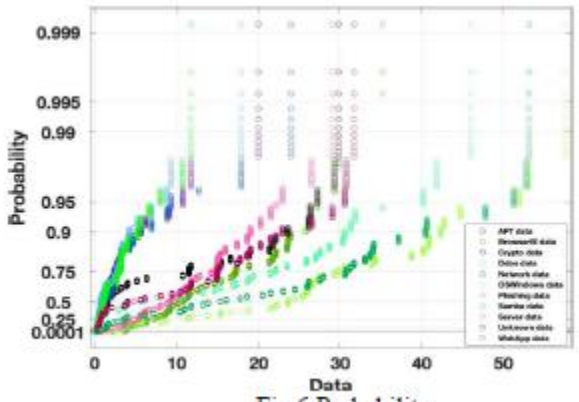


Fig.6 Probability

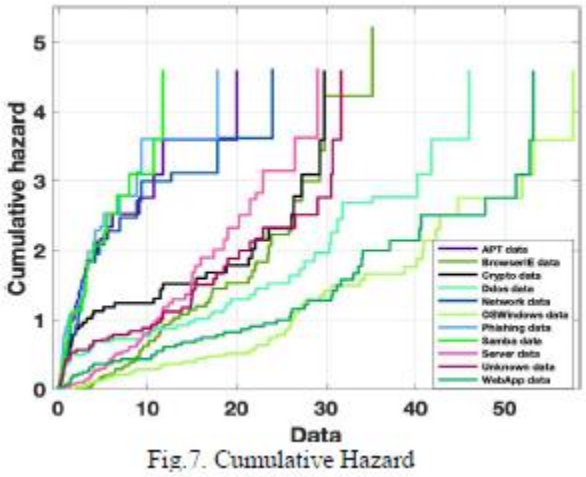


Fig.7. Cumulative Hazard

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

VII. CONCLUSION

There has to be a heightened focus on smart grid cyber security problems due to 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. Nevertheless, guaranteeing the security of every single device inside a DAS is both technically unnecessary and economically inefficient. An innovative method for discovering and ranking DAS vulnerabilities is offered in this paper. 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. How practical and reliable the proposed vulnerability is Case studies based on RBTS bus 2 are offered in this article to demonstrate the evaluation technique.

REFERENCES

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

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

ISSN:2454-9940
www.ijsem.org
Vol 19, Issue.1 March 2025

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

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

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

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

[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] 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] 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] 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] 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] 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.