International Journal of Engineering and Management Research e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-3 (June 2023)
https://ijemr.vandanapublications.com https://doi.org/10.31033/ijemr.13.3.1

Cyber Security Analysis in Cyber Defense for DrNGPASC in Coimbatore City

Dr. N. Vanitha
Associate Professor, Dr. N.G.P. Arts and Science College, Coimbatore, INDIA

Corresponding Author: vanitha@drngpasc.ac.in

Received: 01-05-2023 **Revised:** 18-05-2023 **Accepted:** 30-05-2023

ABSTRACT

Cybersecurity is a progressively vital concern in today's advanced age. With the expanding utilize of innovation in different segments, cyber assaults have gotten to be more modern and broad, posturing a critical danger to people, organizations, and governments. Cyber defense is vital in securing against these assaults, and cyber security examination plays a key part in creating compelling defense techniques. This paper presents a comprehensive investigation of cyber security within the setting of cyber defense. It analyses the different sorts of cyber assaults and the procedures utilized by cyber criminals to breach security frameworks. It moreover audits the current state of cyber defense methodologies and innovations, highlighting their qualities and shortcomings. The paper proposes a system for cyber security examination in cyber defense, which incorporates distinguishing potential dangers, surveying their affect, and creating fitting defense methodologies. The system consolidates an extend of strategies, counting hazard appraisal, defencelessness investigation, and occurrence reaction arranging in Dr. N.G.P. Arts and Science College, Coimbatore. The discoveries of this work paper recommend that cyber security investigation may be a critical component of cyber defense, which a proactive approach is required to successfully relieve the dangers postured by cyber assaults. The system proposed in this paper gives a valuable device or organizations and governments to create viable cyber defense methodologies and secure against cyber dangers.

Keywords-- Cyber Security, Cyber Defense, Security Analysis

I. INTRODUCTION

Nowadays, cybersecurity is an essential concern in this digital age. With the increasing use of technology in various sectors, cyber-attacks have become classier and widespread, posing a major threat to individuals, organizations, and governments. Cyber defense is crucial in protecting against these attacks, and cyber security analysis plays a key role in developing effective defense strategies. By examining these key features of effective cyber defense, this paper tries to find and provide insights and commendations to help societies to strengthen their defenses and mitigate the hazards impersonated by cyber threats. The paper also highlights the importance of cybersecurity training and awareness for employees and stakeholders, as well as the value of established cybersecurity frameworks like NIST Cybersecurity Framework and ISO/IEC27001 in guiding organizations in implementing effective cyber defense strategies. Furthermore, the paper explores emerging areas in cyber defense such as supply chain security, IoT security, and incident reporting and information sharing, and discusses their potential implications for organizations. Overall, this paper underscores the critical need for proactive and comprehensive cyber defense strategies in the face of ever-evolving cyber threats. By analyzing the various features of effective cyber security analysis and exploring emerging trends in the field, this paper targets to offer a footing for continued research and development in this crucial area of information technology.

1.1 Problem Statement

To learn about educational Institution's cybersecurity defenses and the use of Cyber Security analytics to become more efficient in spotting the patterns that symbolize network threats. In addition, the study looks at the alertness among students of IT in educational institutions about the new data management and analytic technologies now available to help educational institutions become more proactive and intelligent about detecting and stopping threats.

1.2 Objectives

The objective of this research work is to deliver a widespread assessment of the present state of cyber defense strategies and propose effective measures to enhance the Dr. N.G.P. Arts and Science College's effectiveness. The study will identify the key challenges faced by the institution in defending against cyber-attacks and propose effective solutions to mitigate them.

II. BACKGROUND STUDY

Narus Validation from Ponemon Institute LLC (2013) conducted an independent study on Bigdata Analytics in Cyber Defense. In this study, 706 IT and IT security professionals with an average of 10 years' experience were polled. They worked in financial services, manufacturing, and government. Each respondent has some degree of responsibility for overseeing the organization's defence against cyber security assaults. They are all aware of their

organization's defence against such attacks. The work is supported by the TERADATA, Ponemon Institute LLC, United States.

Lidong Wang and Randy Jones (2019), analysed the various datasets with different data types like categorical data and numerical data and performed Data duplicates detection and removal, missing values detection, and data quality analysis. Performed the correlation analysisof variables and a clustering analysis based on k-means.

Hathaway et al., 2012 and Rossini et al,2014 discussed about how a hurdle to improving their comprehension of the concept is the lack of a clear unity for cyber-attacks. There won't be coherence in the pieces if the overall isn't coherent. Senior corporate leaders, representatives of the government, and academics are aware that: I) significant financial and legal costs associated with cyberattacks.ii) vulnerabilities in high-value assets such as supervisory- control and data-acquisition systems (Ashford, 2013; Crawford, 2014; Kovacs, 2014; Nicholson et al., 2012; Weiss, 2014); iii) concerns about the upcoming deployment of the "Internet of Things" (IoT) (NSTAC, 2014); and iv) few constraining mechanisms to inhibit malicious behaviours of threat actors (Castel, 2012; Jowitt, 2014, Scully, 2013; Sugarman, 2014; Weiss, 2014).

This study on cyberattacks use the inductive reasoning method and makes use of publicly available data on cyberattacks from sources thought to be trustworthy. The methodology employed in this study to define the term "cyber-attack" is comparable to the methodology utilised in the late 1990s to define the term "security" (e.g., Baldwin, 1997; Buzan, 1998; Huysmans, 1998). Researchers in security developed key characteristics to define what security actually meant. They removed any doubts or discrepancies between the many applications of the security concept. Table 1 shows the literatures reviewed.

Table 1: Literature Review

S.No.	Author	Journal and Year published	Techniques	Observation
01	M.A.Alghamdi & A.Alenazi	Network and computer application	Artificial Intelligence	Inclusive language acknowledges diversity, conveys respect to all people, is sensitive to differences, and promotes equal opportunities. Content should make no assumptions about the beliefs or commitments of any reader
02	Kumar.S & Sharma.R	Computer science and mobile computing	Machine Learning	we have presented a method of feature extraction for handwritten character recognition. We showed that our method, despite its simplicity, yields good classification results on handwritten characters. Normalization and binarization are the pre-processing techniques used for getting accurate results
03	Sood.S.K & Enbody.R.J	Cybe Security Technology	Threats and Teachnology	Cybersecurity incidents and attacks have become almost daily news, and two new surveys give voice to the executives and cybersecurity professionals struggling to defend their organizations.

III. RESEARCH GAPS IDENTIFIED

These omissions include information security policy, detection, containment, personnel training, and vulnerability management. The act of identifying weaknesses in the computer systems and putting security measures in place to counter them is known as vulnerability management. Security flaws are most typically found in a company's auxiliary operations. For instance, a company that handles the servicing of product warranties may do a terrific job at it, but it may not be aware that it is holding credit card information in unencrypted documents.

IV. MATERIALS AND METHODS

Coverage of the study is limited to Dr. N. G.P. Arts and Science College, Coimbatore, Tamil Nadu. The study concentrates on IT department students in Dr. N. G.P. Arts and Science College of Tamil Nadu. Random sampling method is used. Data Collection done through Web based Survey. Figure 1 shows the flow of work done.

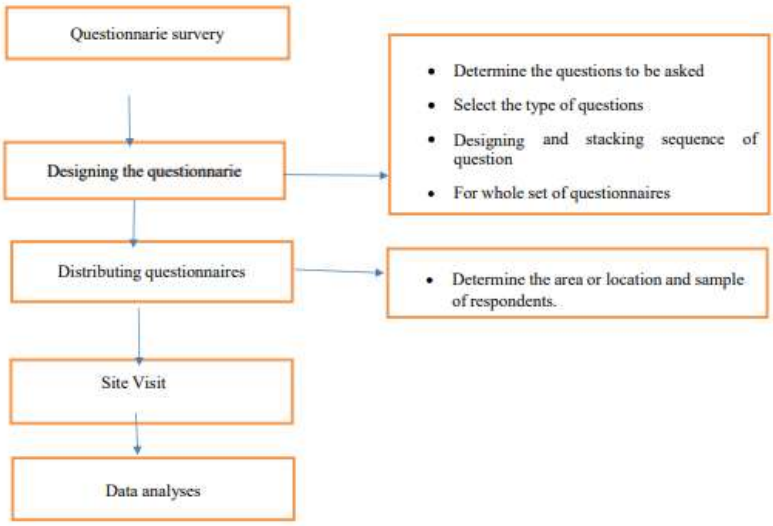

Figure 1: System flow of research work

Data from web-based survey with various data types including numerical data and categorical data are analyzed with the help of R Programming and its functions. Data duplicates detection and removal, missing values detection, and data quality analysis are also performed. Many redundancies can be detected by correlation analysis. A strong correlation between two variables indicates that they have much overlapping information and one of them can be removed.

Steps to carry out the study is given below,

1. Prepare Questionnaire
2. Web-based survey
3. Clean and Analyse the data using R programming
4. Results and Suggestions

Figure 2 shows the methodology of the work done to complete this cyber security analysis towards cyber defense.

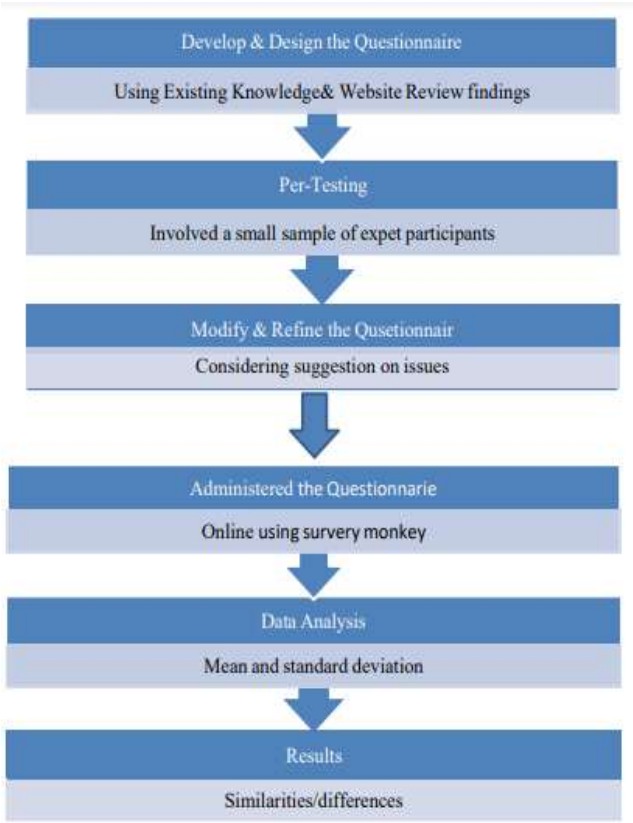

Figure 2: Methodology

V. RESULTS AND DISCUSSIONS

According to the details collected from the students, the most effective cyber security analysis technique they aware of is Vulnerability Scanning and Management then Network Security Monitoring (NSM), Malware Analysis and Reverse Engineering at last Forensic Analysis and Incident Response and others. Figure 3 shows the results of most effective cyber security analysis techniques.

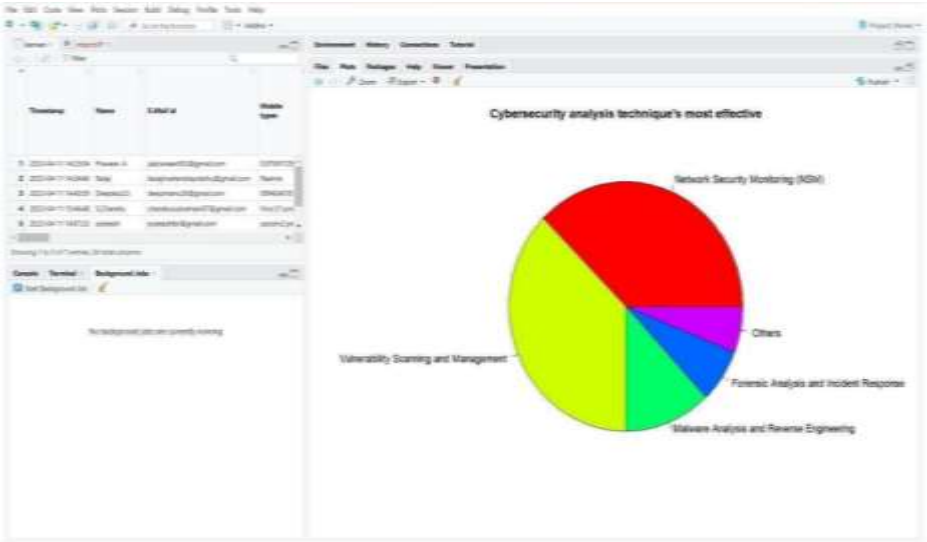

Figure 3: The most effective cyber security analysis technique

Students response for how frequently does the organization conduct cybersecurity analysis is ranked as Daily, Weekly, Monthly, Quarterly, Annually. Most of the students responded as monthly analysis and the lest response is for daily. The results form student's response is depicted in the Figure 4.

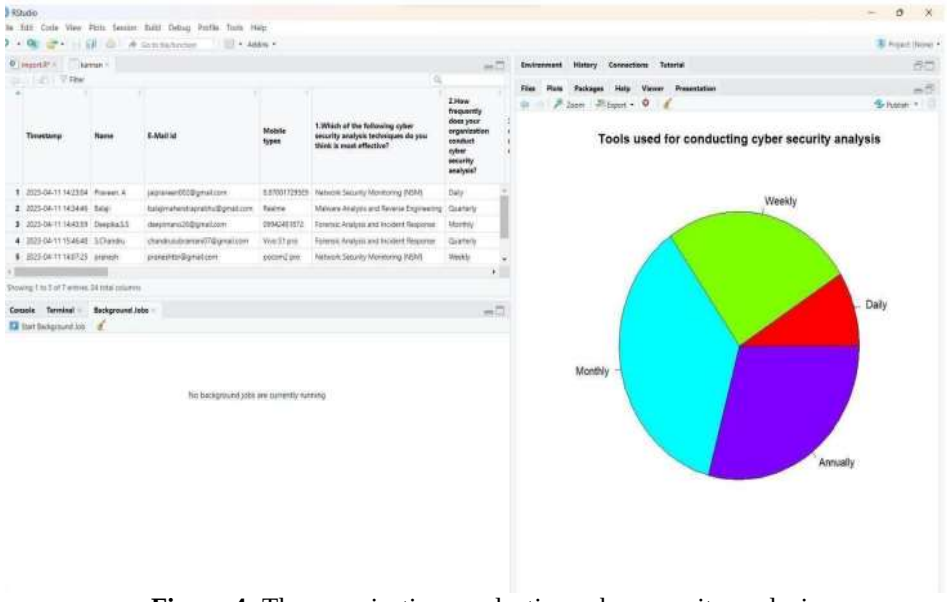

Figure 4: The organization conducting cyber security analysis

The authentication methods used by the organization is recorded as Password, Biometric and multifactor. Students raked it as biometric, password, multifactor and others. Results are shown in the Figure 5.

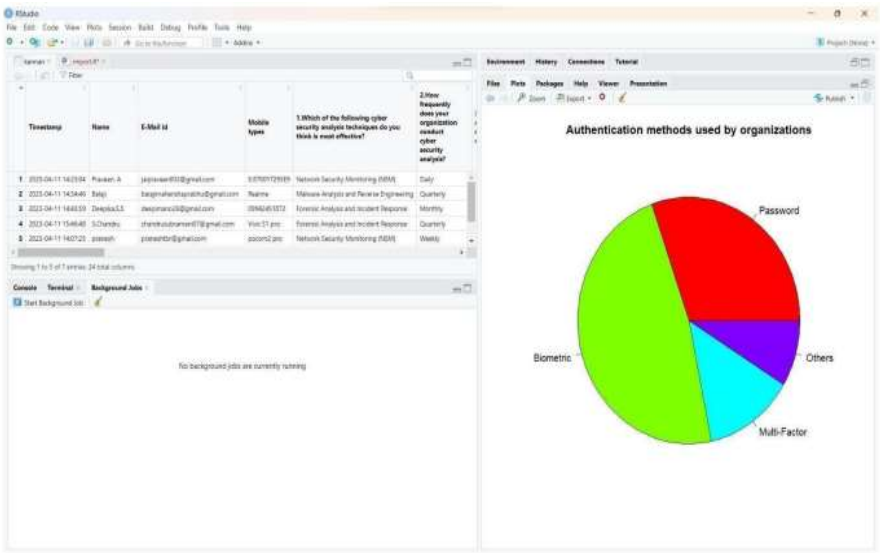

Figure 5: Authentication method used by the organization

The most prominent threat faced by the organisation is recorded as Ransomware and the DoS attack. Phishing, APT and other threats are least identified. Figure 6 shows the students response that the most prominent threat identified by the organisation.

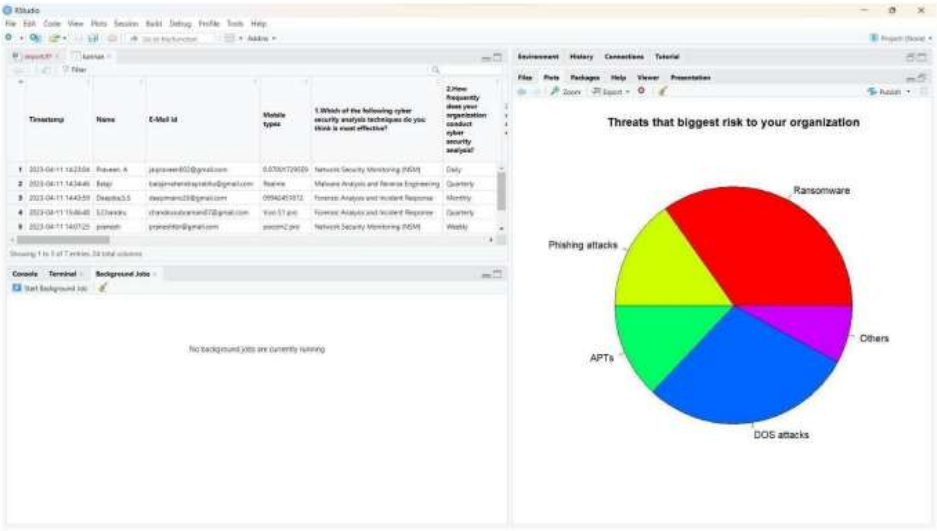

Figure 6: Threats faced by organization

VI. CONCLUSION AND FUTURE WORK

Cyber security analysis is a critical component of cyber defense, and organizations must take a proactive and holistic approach to protect their systems, data, and reputation. By implementing a range of strategies and technologies, such as threat hunting, identity and access management, SIEM, and forensic analysis, organizations can better safeguard themselves against the growing threat landscape. However, it is important to note that cyber security is a constantly evolving field, with new threats and technologies emerging all the time. As such, organizations must remain vigilant and adapt their security practices to keep pace with the evolving threat landscape. By staying up-to-date with the latest developments in cyber security, and by prioritizing a proactive approach to defense, organizations can better protect themselves against the growing threat of cyber attacks.

REFERENCES

[1] Aloulou, M. A., Alghamdi, A. A. & Alenazi, A. (2019). Cybersecurity challenges and solutions:

A review. *Journal of Network and Computer Applications, 131*, 1-26.

[2] Arora, S. & Gupta, M. (2018). Cyber security threats and challenges: A review. *Procedia Computer Science, 132*, 1353-1361.

[3] Kumar, S. & Sharma, R. (2020). A review of cyber security threats and solutions. *International Journal of Computer Science and Mobile Computing, 9*(5), 45-52.

[4] Li, F., Zou, C. & Lou, W. (2019). A survey of cyber security technologies. *IEEE Communications Surveys & Tutorials, 21*(3), 2702-2733.

[5] Mukherjee, S. & Chakraborty, S. (2020). Cyber security: A review of the stateof-the-art. *Journal of Network and Computer Applications, 149*, 102475.

[6] Shrivastava, P. & Mishra, D. (2020). Cyber security: A review of challenges and solutions. *Journal of Cybersecurity and Privacy, 1*(2), 47-56.

[7] Sood, S. K. & Enbody, R. J. (2019). Cyber security: Threats and solutions. *Journal of Cyber Security Technology, 3*(1), 1-20.

[8] Venkatesan, R. & Vimal, K. E. (2018). A review on emerging trendsin cyber security. *Procedia Computer Science, 132*, 1307-1314.

[9] Wueest, C. & Chien, E. (2018). The cyber security landscape in 2018: Insights from the Symantec Global Threat Intelligence Report. *Symantec Corporation*.

[10] Zhang, X., Du, W., Li, J. & Li, T. (2018). Cyber security: Current trends and future directions. *Journal of Cyber Security Technology, 2*(2), 79-87.

[11] Vanitha, N. & Padmavathi, G. (2018). A study on various cyber-attacks and their classification in UAV assisted vehicular ad-hoc networks. In: *Ganapathi, G., Subramaniam, A., Graña, M., Balusamy, S., Natarajan, R., Ramanathan, P. (eds) Computational Intelligence, Cyber Security and Computational Models. Models and Techniques for Intelligent Systems and Automation. ICC3 2017. Communications in Computer and Information Science, 844*. Springer, Singapore. https://doi.org/10.1007/978-981-13-0716-4_11

Acknowledgement

The work was supported and funded by Dr. N.G.P. Arts and Science College, Coimbatore, Tamil Nadu, India.