Educational Administration: Theory and Practice
2024,30(3), 2616 - 2622
ISSN:2148-2403
https://kuey.net/
Research Article

Smart Secure Insight Analyzer

Vanshita Jain[1*], Rachita Samant[2], Hetavi Mehta[3], Sridhar Iyer[4]

[1*]Department of Computer Engineering DJSCE Mumbai,India Email:- vanshitajainofficial@gmail.com
[2]Department of Computer Engineering DJSCE Mumbai,India Email:- rachitasamant77@gmail.com
[3]Department of Computer Engineering DJSCE Mumbai,India Email:- hetavidm22@gmail.com
[4]Department of Computer Engineering DJSCE Mumbai,India Email:- sridhar.iyer@djsce.ac.in

Citation: Vanshita Jain, (2024), Smart Secure Insight Analyzer *Educational Administration: Theory and Practice*, *30*(3), 2616 - 2622
Doi: 10.53555/kuey.v30i3.7274

ARTICLE INFO **ABSTRACT**

Organisations face an unprecedented amount of cybersecurity threats in today's quickly changing digital ecosystem, which poses serious hazards to their operations and data protection. It is therefore extremely important to proactively identify and mitigate these dangers in order to protect sensitive assets and ensure business continuity. In light of the current situation, this research study highlights the significance of Cyber Threat Intelligence (CTI) generation and the necessity of thorough analysis and correlation approaches. Through the use of newer technologies and techniques, such as OWASP ZAP and InternetDB Application Programming Interfaces (APIs), the proposed solution is able to collect comprehensive digital footprints of target sites. By means of correlation with a variety of datasets, including the Common Weakness Enumeration (CWE) dataset and OWASP ZAP dataset, stakeholders are able to obtain significant insights into the dynamic threat landscape.

This research emphasises the value of efficient CTI generation in enabling enterprises to proactively counteract cybersecurity risks, adjust to the ever-changing threat landscape, and maintain resilience in the face of new obstacles.

Index Terms—Cybersecurity Threats, Cyber Threat Intelligence (CTI), Digital Footprints, Comprehensive Analysis, Correlation Techniques, Application Programming Interfaces (APIs), InternetDB, OWASP ZAP.

I. INTRODUCTION

Cybersecurity risks are ever-evolving, posing a threat to organisations in today's hyperconnected digital landscape. Ensuring the security and integrity of sensitive data and systems requires the ability to identify, evaluate, and counteract these risks. Organisations rely on Cyber Threat Intelligence (CTI) to provide them with actionable insights into potential threats and vulnerabilities.

Cyber Threat Intelligence (CTI) encompasses the methodologies of collecting, analyzing, and distributing information regarding cybersecurity risks and the threats facing organizations. The creation of threat reports, which give organisations thorough evaluations of both existing and new risks along with suggestions for mitigation techniques, is a crucial part of CTI. These reports are a great resource for organisations to help them prioritise security activities, comprehend the threat landscape, and make well-informed decisions to safeguard their assets.

Advanced technologies, methodology, and skills are needed by organisations to provide insightful threat reports and implement a successful CTI programme. In order to gather and analyse enormous volumes of data from diverse sources, including network logs, open-source intelligence (OSINT), and proprietary threat feeds, this entails utilising automated techniques and technologies.

Additionally, in order to spot patterns and trends that point to possible dangers, organisations must use powerful analytical tools like machine learning and correlation analysis.

Enhancing CTI capabilities also requires cooperation and information exchange throughout the cybersecurity sector. Organisations can have access to a plethora of collective knowledge and experience through participation in threat intelligence sharing initiatives and industry peer collaboration. This empowers them to more effectively predict and respond to new threats.

When summed up, threat reports and CTI are essential parts of a contemporary cybersecurity strategy because they give businesses the knowledge and understanding they need to keep ahead of changing threats and defend against online attacks. Organisations may create proactive defences and sustain resilience in the face of increasingly complex cyberthreats by utilising cutting-edge tools, processes, and cooperation.

II. LITERATURE SURVEY

In the evolving era of cybersecurity, it was important to carry out thorough literature survey to understand the research gap and introduce betterments in field of threat intelligence. Below are some of the papers we studied to understand and improve the threat detection and intelligence sector of cyber security.

The extensive literature survey presented encapsulates a broad spectrum of strategic advancements and innovations within the cybersecurity field, underscoring a significant shift toward proactive measures in managing and mitigating cyber threats. Initially, paper [1] emphasizes the refined application of the Common Vulnerability Scoring System (CVSS), proposing enhancements that tailor the prioritization of cybersecurity efforts to better suit the unique dynamics of organizational network environments. Complementary insights from paper [2] explore the evolution of vulnerability assessment tools like Nessus and Netsparker, which facilitate less intrusive and more sophisticated data gathering, pivotal for crafting effective security management strategies. In the realm of Cyber Threat Intelligence (CTI), both papers [3] and [6] bring to focus the pressing challenge of information overload—a consequence of the vast CTI sharing via Open Source Intelligence sources. These papers argue the potential of natural language processing as a transformative tool to refine the analysis and streamline the dissemination of critical CTI, enhancing its utility and actionability. Shifting focus on operational security, paper [4] discusses the development of nuanced security metrics that utilize CVSS ratings to systematically classify and prioritize vulnerabilities. This is essential for bolstering organizational defenses by aligning resource allocation with the severity of potential threats. Simultaneously, paper [5] probes into vulnerabilities specific to web applications, highlighting the limitations of current scanning technologies such as OWASP ZAP, particularly in their ability to navigate the complexities of modern web architectures like single-page applications. It advocates for tailored improvements that enhance detection capabilities, thereby reducing exposure to common exploits such as SQL injections and cross-site scripting.

Further dissecting the role of technology in cybersecurity, paper [7] documents the significant edge that machine learning—and specifically deep learning—offers over traditional security methods in the detection of cyber threats. This technological prowess not only enhances the identification of threats like phishing and malware but also optimizes the overall costeffectiveness of cybersecurity operations. Addressing another niche yet critical aspect of cybersecurity, paper [8] delves into the nuanced challenges associated with detecting AuthCross-Site Request Forgery (CSRF). The paper suggests that a combination of robust experimental research along with advanced natural language processing techniques could pave the way for more efficient recognition and analysis of these complex threats. Paper [9] emphasizes the potential for revolutionizing Next-Generation Security Operations Centers (NGSOCs) through the systematic consolidation and analysis of vast arrays of CTI utilizing cutting-edge data mining and machine learning strategies. This approach promises enhanced predictive accuracy and timely alert systems to mitigate potential threats proactively. Touching upon data management in cyber risk contexts, paper [10] reviews the paradox of vast yet underutilized datasets within the cybersecurity domain, proposing refined data analysis methodologies to aid researchers and the insurance sector in better navigating the cybersecurity landscape.

The innovative CyVIA framework introduced in paper [11] exemplifies an integrative approach to cyber threat analysis, aiming to elevate the precision in identifying network vulnerabilities through a cohesive synthesis of threat data from various sources. This system not only identifies but also categorizes vulnerabilities, thereby facilitating more targeted mitigation strategies. Technological foresight continues with paper [12], which investigates the potential of Natural Language Processing (NLP) to forecast CVSS ratings from vulnerability descriptions, aiming to enhance model accuracy through strategic data manipulation and preprocessing techniques. Lastly, paper [13] returns to the foundational concern of vulnerability management within IT networks. By advancing specific methodologies focused on the effective prioritization of vulnerabilities, this research underscores the crucial need for precise management practices that are not only reactive but predictive in nature, ensuring that cybersecurity protocols evolve in tandem with emerging technological landscapes and threat vectors.

The literature surveyed reveals several shortfalls across the discussed papers. Paper [1], while it advances the use of the Common Vulnerability Scoring System (CVSS), could further detail practical implementation challenges in diverse network environments. Papers [3] and [6], advocating for the use of natural language processing in Cyber Threat Intelligence (CTI), do not completely address the accuracy and reliability concerns with automating threat information extraction, which could affect the quality of the data processed. The methods proposed in paper [4] for prioritizing vulnerabilities using CVSS ratings might overlook emerging threats that have not yet been sufficiently documented in existing databases like NVD, potentially leading to gaps in security coverage. Although paper [5] seeks improvements in web application scanners like OWASP ZAP, there remains a need for a broader analysis on the adaptability of these tools to new web technologies beyond single-page applications. Similarly, while the application of machine learning in cybersecurity is promising as discussed in paper [7], these approaches require extensive datasets for training, which may not always be readily available or may be biased, hence impacting the effectiveness of threat detection systems. Additionally, the proposed solutions for Auth-CSRF in paper [8] lack discussions on scalability and real-world application to a variety of web architectures. Lastly, while papers like [13] emphasize improved methodologies for vulnerability prioritization, these often rely heavily on quantitative data assessments, potentially overlooking qualitative insights from seasoned cybersecurity professionals which can be critical in nuanced threat contexts. These gaps collectively highlight areas where future research could further refine the effectiveness and applicability of cybersecurity strategies.

To address the identified shortfalls in surveyed literature, it is essential to focus on practical implementation. Which can be mentioned but not limited to expanding vulnerability databases to include emerging threats, concentrating on improving the accuracy and reliability of the machine learning techniques in analyzing cyber threat intelligence.

III. METHODOLOGY

The methodology consists of a methodical approach to the development of Cyber Threat Intelligence (CTI), with a focus on advanced analytical tools, correlation techniques, and digital footprint analysis. By using the OWASP ZAP and InternetDB APIs, domain data is gathered and vulnerabilities are found by spidering susceptible websites. Data about vulnerabilities is built into a new database and compared with digital footprints.

Using an 88 percent accurate Random Forest model improves pattern recognition and makes it possible to identify possible dangers. The next step is to map vulnerabilities using the Common Vulnerability Scoring System (CVSS) and provide reports so that stakeholders may make educated decisions.

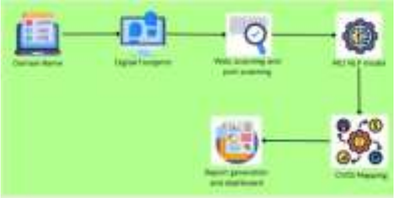
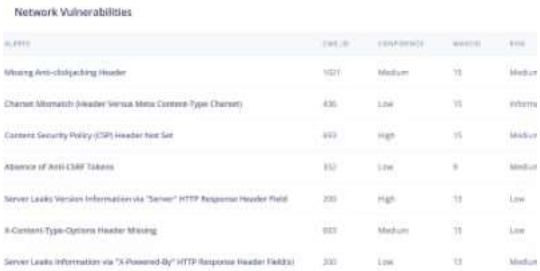

Domain Name
Digital Footprint
Web Scanning and port scanning
ML/ NLP model
CVSS Mapping
Report generation and dashboard

Fig. 1. System Architecture

A. Digital Footprint

To gather domain-specific data, run vulnerability scans with the OWASP ZAP API. Concentrate on locating security holes, open ports, and other parts of network reconnaissance in the target domain's infrastructure. The OWasp zap API gives the 20 different vulnerability details like alert, alertref, confidence, cweid, description, evidence, id, inputVector, messageId, method, name, other, param, pluginId, reference, risk, solution, sourceid, tags, url, wascid. From which after cleaning the data we selected alert, cweid, risk, confidence, risk as attributes to train our model on.



Network Vulnerabilities

ALERTS	CWE ID	CONFIDENCE	WASCID	RISK
Missing Anti-clickjacking Header	1021	Medium	15	Medium
Charset Mismatch (Header Versus Meta Content-Type Charset)	436	Low	15	Informa
Content Security Policy (CSP) Header Not Set	693	High	15	Medium
Absence of Anti-CSRF Tokens	352	Low	9	Medium
Server Leaks Version Information via "Server" HTTP Response Header Field	200	High	13	Low
X-Content-Type-Options Header Missing	693	Medium	15	Low
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	200	Low	13	Medium

Fig. 2. Digital footprint details

B. Creation of new database

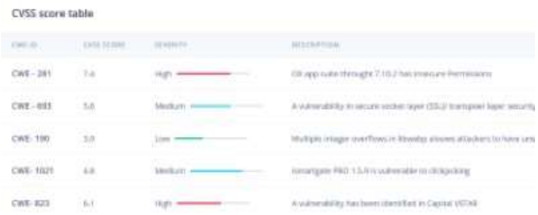
- Spider vulnerable websites : Spidering vulnerable websites is made easier by using the OWASP ZAP API. Navigating through web pages to find connections, forms, and other resources is part of this dynamic investigation. The API allows for the thorough collecting of vulnerability data, including potential attack vectors and security flaws, by methodically scanning through these websites.
- Novelty: One innovative aspect of our project is creation of new dataset, through the literature survey we understood that there is lack of dataset to train our machine learning model hence we created a vulnerability dataset with the help of OWASP ZAP API. To creat new dataset we have used two function getAlerts and fetchAlerts, getAlerts function is used for attacking various testing website namely testphp, bWapp, google Gruyere etc. to obtain information such as alert, confidence, cweid, description, evidence, id, param, pluginId, risk, sourceid, tags, url, wascid, etc. Which was then fetched in JSON format by using fetchAlert function. The JSON format is converted into CSV format for later use. This step helped us in our further correlation process and for extracting meaningful information.

C. Correlation Analysis

The dataset is subjected to advanced analytical approaches such as correlation analysis and machine learning algorithms in order to detect patterns, trends, and anomalies. Making use of an 88 percent accurate Random Forest model improves pattern recognition capabilities, making it possible to identify new risks and subtle correlations. Through a proactive and thorough analytic process, possible threats and vulnerabilities are identified based on information gathered from various sources.

D. CVSS Mapping

Threat assessment: Mapping threats and vulnerabilities found in the integrated dataset to the Common Vulnerability Scoring System (CVSS) scores that correspond to them is the procedure. Based on variables like exploitability, impact on confidentiality, integrity, and availability, as well as complexity, this assessment gives each threat a number score. To map CVSS for threat analysis CWE ids are used. Single CWE id has more than one threats identification associated with it. Hence while mapping the average of cwe id with its severity and impact in taken into consideration. Through the utilisation of the CVSS framework, entities can effectively manage and mitigate risks by ranking and categorising threats based on their level of severity.



CVSS score table

CWE ID	CVSS SCORE	SEVERITY	DESCRIPTION
CWE - 281	7.6	High	Git app suite through 7.10.2 has insecure Permissions
CWE - 693	5.6	Medium	A vulnerability in secure socket layer (SSL)/ transport layer security
CWE- 190	3.0	Low	Multiple integer overflows in libwebp allows attackers to have uns
CWE- 1021	4.8	Medium	[illegible] P60 1.5.0 is vulnerable to clickjacking
CWE- 823	6.1	High	A vulnerability has been identified in Capital VSTAR

Fig. 3. CVSS Mapping

E. Summary Report and Dashboard

- Report generation : The obtained data from whole process and CVSS mapping are presented in a thorough summary report . This report consolidates the analysis findings. This comprehensive report gives users the knowledge they need to take educated decisions about cybersecurity solutions. Together with suggestions for risk-reduction tactics based on the evaluated risks, the report provides statistics on the frequency and seriousness of threats that have been discovered.
- Dashboard enhancement : To go along with the summary report, a user-friendly dashboard interface is created that presents the analysis metrics and visualisations in an easy-to-read manner. With interactive tools like dynamic charts, graphs, and tables, stakeholders may efficiently examine and analyse cybersecurity intelligence within the dashboard. Users are able to evaluate the efficacy of mitigation measures that have been put in place, track security trends over time, and obtain insights into new threats using the dashboard. In general, the interactive dashboard and summary report work together to improve situational awareness and provide stakeholders with the resources they need to manage cybersecurity risks.

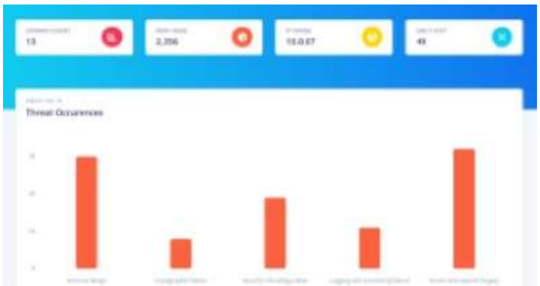


Fig. 4. Dashboard page

IMPLEMENTATION

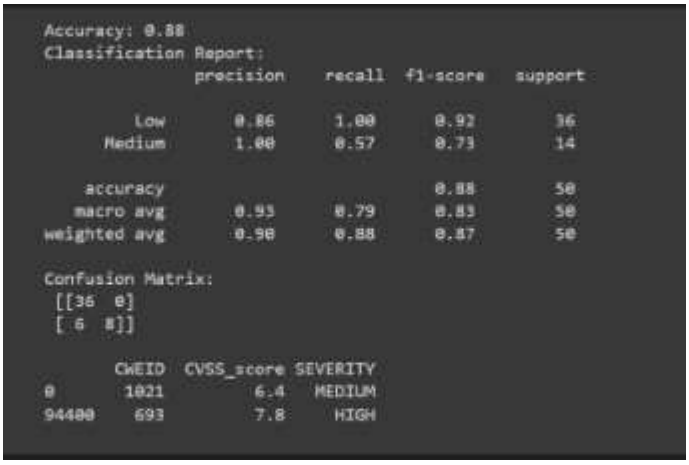
In implementation, we start by examining the user input in form of website url, the url is used in digital footprint process where the domain's online activities and its characteristics are gathered through the utilization OWASP ZAP API. The url acts as the central starting point for the detailed domain examination. The results of digital footprint are collection of network details as well as vulnerability details which form a solid foundation for an in-depth analysis.

Moving forward, a dataset is constructed using OWASP ZAP API, which is specifically designed to simulate attacks on various websites to gather comprehensive network details . The network details contain 20 different data attributes which were then cleaned and important attributes were selected for making the dataset. This dataset serves as a crucial resource for correlation purposes. The main intent here is to use this information for cross-referencing and enhancing the understanding of potential threats.

The extracted digital footprint from the domain name is then correlated with newly formed dataset and the established CWE (Common Weakness Enumeration) database to extract pertinent insights. The purpose of this correlation is to discern patterns that reveal the probabilities of various types of cyberattacks. These probabilities are quantified and presented as percentages, representing the likelihood of each type of threat occurring.

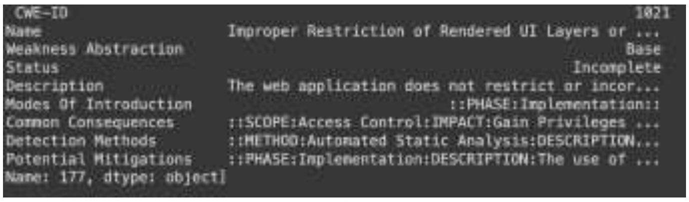
To further enhance the analysis, the mapped results are compared with CVSS scores for a thorough impact analysis. This comparison provides a more nuanced view of the potential impact of each identified threat, helping to prioritize the threats in terms of their potential damage.

Finally, the collection of this analysis is presented through an intuitive dashboard interface which presents the scrutinized data in a visually appealing manner, allowing stakeholders to effortlessly grasp its significance. Additionally, a CTI (Cyber Threat Intelligence) report is generated, consolidating the insights gleaned from the analysis into a comprehensive document. This approach ensures the efficient extraction of actionable intelligence and facilitates informed decision-making in mitigating potential cyber security threats.



```
Accuracy: 0.88
Classification Report:
               precision    recall  f1-score   support

         Low       0.86      1.00      0.92        36
      Medium       1.00      0.57      0.73        14

    accuracy                           0.88        50
   macro avg       0.93      0.79      0.83        50
weighted avg       0.90      0.88      0.87        50

Confusion Matrix:
 [[36  0]
 [ 6  8]]

       CWEID  CVSS_score SEVERITY
0       1021         6.4   MEDIUM
94400    693         7.8     HIGH
```

Fig. 5. CVSS output



```
 CWE-ID                                                          1021
Name                    Improper Restriction of Rendered UI Layers or ...
Weakness Abstraction                                             Base
Status                                                     Incomplete
Description             The web application does not restrict or incor...
Modes Of Introduction                      ::PHASE:Implementation::
Common Consequences     ::SCOPE:Access Control:IMPACT:Gain Privileges ...
Detection Methods       ::METHOD:Automated Static Analysis:DESCRIPTION...
Potential Mitigations   ::PHASE:Implementation:DESCRIPTION:The use of ...
Name: 177, dtype: object]
```

Fig. 6. Correlation output

FUTURE SCOPE

The cybersecurity field is very vast with constantly changing landscapes of cyber attacks therefore this future underlines the ambition to expand beyond traditional vulnerability assessment method into more proactive and dynamic cybersecurity practices.

- Automated Security Monitoring (ASM) Integration: Link the system to Automated Security Monitoring (ASM) programmes to allow for ongoing observation of the company's digital assets. ASM improves threat detection capabilities and shortens response times by automating the detection and response to security incidents in realtime, strengthening the organization's cybersecurity posture.
- Red Teaming Integration: Integrate Red Teaming techniques into the system, making use of automated tools to test the organization's defences against modern threats and imitate complex cyberattacks. Organisations may proactively find and fix vulnerabilities, fortify their defences, and enhance their readiness for incident response by automating the Red Team exercise process.
- Enhanced Attack Automation: Increase the system's capacity to automate more cyberattacks, such as targeted social engineering attacks, advanced persistent threats (APTs), and zero-day exploits. Organisations can test their defences against skilled attackers and replicate intricate attack scenarios by utilising modern attack automation tools.
- Integration with Threat Intelligence Platforms (TIPs): To expedite the gathering, processing, and distribution of threat intelligence data, integrate the system with Threat Intelligence Platforms (TIPs). Utilising TIPs, businesses may automate threat intelligence stream aggregation, correlate insights that are actionable, and plan reaction measures to successfully manage cyber attacks.

CONCLUSION

In summary, the creation of a state-of-the-art system for generating cyber intelligence threat reports signifies a noteworthy advancement in the field of cybersecurity through this project. This research stands out because it uses Random Forest, a powerful machine learning algorithm, to provide a fresh method for threat detection and analysis in the context of cybersecurity. Interestingly, the use of Random Forest in the field of cryptography is a novel advancement because before to now, this specific machine learning model has not been thoroughly investigated within cryptographic frameworks.

Random Forest algorithm, enables system to detect complex patterns and trends in data which boost the correlation and helps the system to improve threat detection's precision and accuracy, giving enterprises a proactive defense against new cybersecurity threats.

Additionally, the digital footprinting and report production processes were made more efficient by the integration of APIs and function calls, which added a layer of automation that drastically decreased the amount of manual labor required. The process of gathering digital footprint via an API combined insights from several analyses made it easier to get data from a variety of sources. This helped to provide thorough and useful threat intelligence reports in addition to speeding up the workflow.

The project provides a paradigm shift in cybersecurity techniques with its creative mix of cryptography, machine learning, and API connections. This innovative strategy has the ability to completely change how businesses handle threat intelligence and strengthen their defenses against constantly changing cyberattacks.

REFERENCES

[1] T. Harada, A. Kanaoka, E. Okamoto and M. Kato, ”Identifying Potentially-Impacted Area by Vulnerabilities in Networked Systems Using CVSS,” 2010 10th IEEE/IPSJ International Symposium on Applications and the Internet, Seoul, Korea (South), 2010, pp. 367-370, doi: 10.1109/SAINT.2010.105.

[2] B. J. Santoso, R. M. Ijtihadie and G. N. S. Aryawan, ”Vulnerability Data Assessment and Management Based on Passive Scanning Method and CVSS,” 2023 14th International Conference on Information and Communication Technology and System (ICTS), Surabaya, Indonesia, 2023, pp. 325-330, doi: 10.1109/ICTS58770.2023.10330884.

[3] Y. Ghazi, Z. Anwar, R. Mumtaz, S. Saleem and A. Tahir, ”A Supervised Machine Learning Based Approach for Automatically Extracting High-Level Threat Intelligence from Unstructured Sources,” 2018 International Conference on Frontiers of Information Technology (FIT), Islamabad, Pakistan, 2018, pp. 129-134, doi: 10.1109/FIT.2018.00030.

[4] A. Tripathi and U. K. Singh, ”On prioritization of vulnerability categories based on CVSS scores,” 2011 6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), Seogwipo, Korea (South), 2011, pp. 692-697.

[5] A. Jakobsson and I. Haggstr¨ om, ‘Study of the techniques used by¨ OWASP ZAP for analysis of vulnerabilities in web applications’, Dissertation, 2022.

[6] R. Marinho and R. Holanda, ”Automated Emerging Cyber Threat Identification and Profiling Based on Natural Language Processing,” in IEEE Access, vol. 11, pp. 58915-58936, 2023, doi: 10.1109/ACCESS.2023.3260020.

[7] S. Sutar, P. Khune, H. Gandhi, K. S. Pattebahadur and C. N. Aher, ”Real Time Network Attack Detection Using Machine Learning Techniques,”
2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-6, doi: 10.1109/ICCCNT56998.2023.10307711.

[8] A. Sudhodanan, R. Carbone, L. Compagna, N. Dolgin, A. Armando and U. Morelli, ”Large-Scale Analysis and Detection of Authentication Cross-Site Request Forgeries,” 2017 IEEE European Symposium on Security and Privacy (Euro S and P), Paris, France, 2017, pp. 350-365, doi: 10.1109/EuroSP.2017.45.

[9] Yang, W., Lam, KY. (2020). Automated Cyber Threat Intelligence Reports Classification for Early Warning of Cyber Attacks in Next Generation SOC. In: Zhou, J., Luo, X., Shen, Q., Xu, Z. (eds) Information and Communications Security. ICICS 2019. Lecture Notes in Computer Science(), vol 11999. Springer, Cham. https://doi.org/10.1007/978-3030-41579-2-9

[10] Cremer, F., Sheehan, B., Fortmann, M. et al. Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract 47, 698–736 (2022). https://doi.org/10.1057/s41288-02200266-6

[11] A. A. Malik and D. K. Tosh, ”Robust Cyber-threat and Vulnerability Information Analyzer for Dynamic Risk Assessment,” 2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom), Athens, Greece, 2021, pp. 168-173, doi: 10.1109/ MeditCom49071.2021.9647584.

[12] J. C. Costa, T. Roxo, J. B. F. Sequeiros, H. Proenca and P. R. M. INACIO, ”Predicting CVSS Metric via Description Interpretation,”´ in IEEE Access, vol. 10, pp. 59125-59134, 2022, doi: 10.1109/ACCESS.2022.3179692.

[13] M. Walkowski, M. Krakowiak, M. Jaroszewski, J. Oko and S. Sujecki, ”Automatic CVSS-based Vulnerability Prioritization and Response with Context Information,” 2021 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Hvar, Croatia, 2021, pp. 1-6, doi: 10.23919/SoftCOM52868.2021.9559094.

[14] Humayun, M., Niazi, M., Jhanjhi, N. et al. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arab J Sci Eng 45, 3171–3189 (2020). https://doi.org/10.1007/s13369-019-04319-2

[15] Diptiben Ghelani, Tan Kian Hua, Surendra Kumar Reddy Koduru. Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. Authorea. September 22, 2022. DOI: 10.22541/au.166385206.63311335/v1

[16] R. A. Nafea and M. Amin Almaiah, ”Cyber Security Threats in Cloud: Literature Review,” 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 2021, pp. 779-786, doi: 10.1109/ICIT52682.2021.9491638.

[17] Muhammed Zekeriya Gunduz, Resul Das, Cyber-security on smart grid: Threats and potential solutions, Computer Networks, Volume 169, 2020,
107094, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2019.107094

[18] Diptiben Ghelani. Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. TechRxiv. September 22, 2022. DOI: 10.22541/au.166385207.73483369/v1

[19] Gunduz, M.Z. and Das, R., 2020. Cyber-security on smart grid: Threats and potential solutions. Computer networks, 169, p.107094.

[20] Ahsan, Mostofa, et al. ”Cybersecurity threats and their mitigation approaches using Machine Learning—A Review.” Journal of Cybersecurity and Privacy 2.3 (2022): 527-555

[21] Aljumah, Abdullah, and Tariq Ahamed Ahanger. ”Cyber security threats, challenges and defence mechanisms in cloud computing.” IET communications 14.7 (2020): 1185-1191

[22] Hussain, Abdulla, Azlinah Mohamed, and Suriyati Razali. ”A review on cybersecurity: Challenges emerging threats.” In Proceedings of the 3rd International Conference on Networking, Information Systems Security, pp. 1-7. 2020

[23] Safitra, M.F., Lubis, M. and Fakhrurroja, H., 2023. Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability, 15(18), p.13369

[24] Manulis, M., Bridges, C.P., Harrison, R., Sekar, V. and Davis, A., 2021. Cyber security in new space: Analysis of threats, key enabling technologies and challenges. International Journal of Information Security, 20, pp.287-311

[25] Snider, K.L., Shandler, R., Zandani, S. and Canetti, D., 2021. Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. Journal of Cybersecurity, 7(1), p.tyab019

[26] Shah, V., 2021. Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats. Revista Espanola de Documentacion Cientifica, 15(4), pp.42-66