Grenze International Journal of Engineering and Technology, June Issue

Advancements in Cyber Threat Prediction using Machine Learning and Deep Learning Techniques

Aman Gogiyan[1], Monika Kalra[2] and Ashok Pal[3]
[1-3]Department of Mathematics, Chandigarh University, India
Email: amangogiyan1235@gmail.com, monikae6383@cumail.in, ashokpmaths.iitr@gmail.com

***Abstract*— Cyberattacks pose a danger to the security and integrity of digital ecosystems, hence proactive defensive measures are required to lower risks and safeguard essential resources. The machine learning (ML) and deep learning (DL) techniques utilized in cyber threat prediction are thoroughly examined in this work. Through a thorough synthesis of the literature, this study explores the state-of-the-art, new trends, and potential futures in cyber threat prediction.**
According to research, a number of machine learning (ML) and deep learning (DL) techniques are employed for cyber threat prediction, including convolutional neural networks (CNNs), recurrent neural networks (RNNs), and graph neural networks (GNNs). The study uses a range of datasets assessment criteria to show the benefits and downsides of various ways for detecting and preventing cyberattacks in various threat scenarios.
The significance of multidisciplinary cooperation, methodological innovation, and ethical concerns in improving the area of cyber threat prediction are among the key conclusions drawn from the literature synthesis. Problems including a lack of data, unequal class distribution, and hostile attacks show up as major roadblocks to the creation of trustworthy and effective prediction models. Future research needs are noted, though, and these include standardizing assessment methods, integrating domain knowledge, and developing strong defenses against adversarial assaults. Overall, the study highlights the importance of sophisticated analytics in boosting cybersecurity resilience and the necessity of constant innovation and adaptation to keep up with changing cyberthreats. Policymakers, researchers, and cybersecurity experts may collaborate to improve the security posture of digital infrastructure and reduce new cyber threats by utilizing the research's insights.

***Index Terms*— Cyber threat prediction, Convolutional neural networks (CNNs), Recurrent neural networks (RNNs), Graph neural networks (GNNs)**

I. INTRODUCTION

In our increasingly interconnected digital world, the rise in cyberthreats poses a severe risk to individuals, organizations, and governments alike. Cyberattacks, which may vary from highly skilled network invasions to malware infestations, have become more frequent, sophisticated, and damaging over time [1]. Traditional cybersecurity techniques, such signature-based detection and rule-based systems, often fail to keep up with these evolving threats [2]. Consequently, there's a growing demand for more adaptable and proactive methods of anticipating and averting cyberattacks.
It has been suggested that deep learning (DL) and machine learning (ML) might enhance cyber threat identification and prediction [3]. By using massive amounts of historical data and extracting intricate patterns and correlations,

Grenze ID: 01.GIJET.10.2.844

ML and DL algorithms are more accurate and efficient than traditional ways for detecting irregularities, identifying malicious actions, and forecasting potential intrusions. These techniques enable prompt and accurate responses to emerging threats, potentially strengthening cybersecurity defenses.

The foundation for applying ML and DL techniques to cyber threat prediction has been laid by earlier studies in this field. Convolutional neural networks (CNNs), for instance, have been shown in tests to be successful in malware detection using network traffic analysis [4]. The aforementioned research highlights the significance of feature extraction and selection methodologies in augmenting the effectiveness of deep learning models in detecting cyber threats. Furthermore, new ensemble learning techniques have been presented that combine several machine learning algorithms to forecast cyberattacks in real-time [5]. These methods have demonstrated benefits in terms of improving forecast robustness and accuracy in dynamic cyber settings.

In the field of machine learning and deep learning-based cyber threat prediction, there are still many challenges to be solved despite these advancements. The dynamic nature of cyber threats, the adversarial nature of attackers, and the scarcity of labeled training data provide ongoing challenges to the development of effective prediction models. To get over these challenges and advance the state-of-the-art in cyber threat intelligence and defense, disciplinary barriers must be crossed by academics, practitioners, and policymakers.

In summary, the rapid evolution and increasing sophistication of cyber threats necessitate the development of innovative anticipatory and mitigation measures. Machine learning and deep learning approaches offer viable choices for bolstering cybersecurity defenses by enabling proactive threat identification and fast reaction mechanisms [6]. By expanding on previous research work, this study seeks to improve the area of cyber threat prediction through a comprehensive evaluation of 120 references. Our study tackles the challenges connected with cyber threat intelligence and defense to deepen our understanding of cyber threats and provide useful recommendations for bolstering cybersecurity resilience in the contemporary digital world.

II. Literature Review

The increasing complexity and frequency of cyberattacks in recent years have highlighted the vital need for sophisticated cybersecurity measures to protect digital infrastructures and assets. To improve threat detection skills, researchers have explored novel approaches and technologies in response to this challenge. This literature survey offers an overview of significant advancements around cybersecurity detection and prevention by emphasizing the main conclusions and research techniques used in different studies.

One significant field of research focuses on using social media platforms, such as Twitter, to gather useful cybersecurity intelligence. In his work" Cyberthreat Detection from Twitter using Deep Neural Networks" in 2018 Dion´ısio et al. [7] presented a novel method for extracting and analyzing cybersecurity data from Twitter feeds using deep neural networks (DNNs). Their solution enhanced efforts to gather cyber threat intelligence by demonstrating excellent accuracy in recognizing security-related tweets and extracting pertinent information using bidirectional long short-term memory networks (LSTMs) and convolutional neural networks (CNNs). Another substantial part of cybersecurity threat detection is identifying anomalies in network traffic data. Radford et al. in 2018 [8] suggested a unique way to detect network traffic anomalies using RNN in their study "Network Traffic Anomaly Detection Using Recurrent Neural Networks". Their algorithm learned semantic and syntactic patterns by tokenizing and compressing network traffic data into sequences, allowing it to detect outlier actions that may indicate possible cyber risks. This methodology is a viable alternative to rule-based systems, which frequently fail to generalize to unforeseen threat patterns.

Furthermore, researchers investigated the effectiveness of ensemble machine- learning approaches in network intrusion detection systems (NIDS). Raihan-Al- Masud and Mustafa's work" Network Intrusion Detection System Using Voting Ensemble Machine Learning" in 2019 [9] developed an ensemble machine learning-based NIDS that detects both known and undiscovered cyber threats. By merging various machine learning algorithms with voting, their suggested approach displayed superior performance to standard methods, giving elevated precision and resilience in threat detection.

The significance of evaluating algorithm performance in real-world contexts was underscored in 2020 by Shaukat et al.'s research titled "Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective" [10] wherein the performance evaluation of machine learning algorithms, such as deep belief networks, decision trees, and support vector machines, was done across a range of cyber threat detection tasks. Subsequently, in 2021 Yeboah-Ofori et al.'s work" Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security" [11] demonstrated the effectiveness of predictive analytics in augmenting supply chain security by utilizing cyber threat intelligence (CTI) in conjunction with machine learning approaches to assess and forecast potential risks inside the cyber supply chain.

In addition to typical machine learning techniques, Sewak et al.'s research titled "Deep Reinforcement Learning in the Advanced Cybersecurity Threat Detection and Protection" in 2022 [12] has looked into the potential of deep reinforcement learning (DRL) in cybersecurity threat detection. They examined the use of DRL in advanced threat detection, demonstrating its usefulness in providing AI solutions for domains that previously required extensive human vigilance. Adding to this corpus of research, He, Ji, and Huang in 2022 published "Illuminati: Towards Explaining Graph Neural Networks for Cyber- security Analysis," [13] which discusses the transparency difficulties of graph neural networks (GNNs) in cybersecurity applications. Their research provides a complete and correct explanatory structure for GNN models, allowing the discovery of key nodes, edges, and features that contribute to cybersecurity predictions. With its increased description accuracy and ease of comprehension for domain specialists, Illuminati shows tremendous promise for boosting the construction of cybersecurity applications that leverage GNNs.

Researchers hope to improve threat identification capabilities and responsiveness to new cyber threats by incorporating DRL approaches. Meanwhile, in 2023 Alcudia'd et al. conducted a study titled "A Deep Learning Methodology for Predicting Cybersecurity Attacks on the Internet of Things" [14] that emphasized reducing security threats in Internet of Things (IoT) networks. They found that combining ML and DL algorithms with balancing approaches like SMOTE can help identify intrusions in IoT networks and improve their security. In 2023, Silvestri et al. [15] conducted a study to analyze vulnerabilities and threats in the healthcare ecosystem. Their work, "A Machine Learning Approach for the NLP-Based Analysis of Cyber Threats and Vulnerabilities of the Healthcare Ecosystem," utilized machine learning models such as XGBoost and BERT neural language model. The study provided valuable insights on managing cybersecurity hazards in healthcare settings.

In 2024, Rajak and Tripathi presented their study titled "DL-SkLSTM Approach for Cyber Security Threats Detection in 5G enabled IIoT" [16]. Their study showcased a DL-SkLSTM-based architecture that outperformed various cutting-edge DL and ML techniques in detecting and classifying cyberattacks on an IIoT dataset that was made publicly available. In 2024, to create a safer environment for learning in the metaverse, Nkoro et al. conducted a study titled "Detecting Cyberthreats in Metaverse Learning Platforms Using an Explainable DNN" [17]. They developed an explainable deep neural network (DNN) that accurately recognizes and mitigates network intrusion attempts in these types of environments. Additionally, in 2024, Kumar et al. presented a study titled "Blockchain and Explainable AI for Enhanced Decision Making in Cyber Threat Detection" [18], which validated the potential of combining blockchain technology with explainable AI (XAI) to strengthen cybersecurity defenses. They presented a blockchain-enabled XAI framework for improving the decision-making process in cyber threat detection in smart healthcare systems. With a focus on addressing emerging cyber threats, the literature survey showcases a variety of methodologies and approaches that demonstrate notable advancements in the use of ML and DL techniques for cyber threat prediction. Collaborative efforts between academia, industry, and policymaking are positioned to drive additional innovation and improvement in cyber threat intelligence and security, despite persistent constraints such as data scarcity and adversarial attacks. This synthesis paves the way for further research and refining of predictive technologies to protect digital ecosystems from cyber threats.

III. METHODOLOGY

This study uses machine learning (ML) and deep learning (DL) approaches to synthesize and analyze the body of research on cyber threat prediction in a methodical manner. The steps included in the methodology are described as follows:

A. *Finding Related Studies:* A comprehensive search strategy is employed to locate relevant research papers, conference proceedings, and scholarly publications addressing cyber threat prediction using ML and DL approaches. Using relevant keywords and Boolean operators, such as "deep learning," "machine learning," and "cyber threat prediction," among others, one may query electronic resources such as IEEE Xplore, ACM Digital Library, PubMed, and Google Scholar. The reference lists of the papers that were gathered are also thoroughly examined in order to locate further relevant research.

B. *Selection and Screening Standards*: Using predetermined inclusion and exclusion standards, the retrieved studies are screened [19]. Studies on cyber threat prediction utilizing ML and DL algorithms that have been published in peer-reviewed journals, conference proceedings, or other academic sources meet the inclusion requirements. research not directly relevant to cyber threat prediction, research with little empirical support, and articles published in languages other than English are also excluded.

C. *Data Synthesis and Extraction*: To gather important details from the chosen studies, such as the author(s), year of publication, research goals, datasets used, techniques used, ML/DL algorithms put into practice, performance metrics assessed, and primary findings, data extraction is carried out methodically. The retrieved

data are combined and arranged thematically in order to find recurring themes, new patterns, and places where the examined research agree or disagree.

D. *Evaluation of Quality*: To guarantee rigor and validity, the quality of the examined studies is evaluated. Methodological robustness, sample size, data quality, openness in reporting, and adherence to ethical standards are a few examples of criteria for evaluating quality [20]. Research papers that exhibit rigorous methodology and offer adequate information are given more weight during the process of synthesis and analysis.

E. *Data Analysis and Interpretation*: Using ML and DL approaches, the combined data are analyzed both qualitatively and quantitatively to extract significant insights [21] and formulate general conclusions about the state-of-the-art in cyber threat prediction. To clarify the benefits and drawbacks of various strategies, spot gaps in the literature, and suggest future lines of inquiry, comparative analysis is carried out.

F. *Ethical Considerations*: The evaluation complies with the ethical standards that guide academic research, which include respecting intellectual property rights, properly attributing sources, and abstaining from plagiarism. All sources are correctly cited, and the original writers are given appropriate credit. Furthermore, ethical concerns about informed consent, confidentiality, and data privacy are adequately recognized and considered during the review process.

The methodology flowchart, shown in Fig.1, explains the methodical process utilized in this investigation to assess several cyber threat prediction techniques. The stages required in finding pertinent research papers, screening and choosing studies, extracting and synthesizing data, determining quality, and evaluating data are all outlined in the flowchart. The methodology section provides more information on how each stage was carefully followed to guarantee the rigor and integrity of the analysis process. This flowchart acts as a visual guide for the methods used in this inquiry, bringing transparency and repeatability to the research methodology.

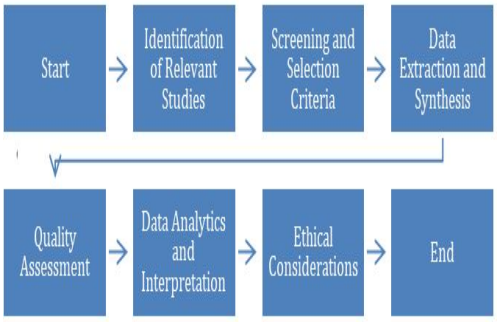

Fig.1 Methodology Flowchart

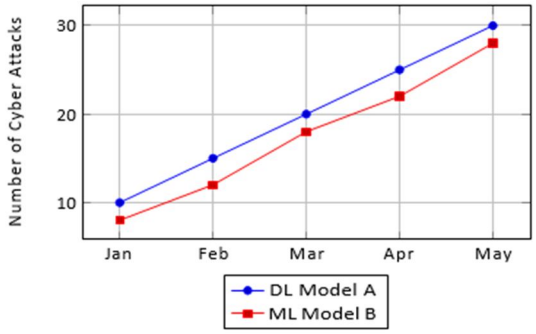

Fig.2 Comparison of Cyber Attacks Detected by ML and DL Models at the Start of 2020

IV. RESULT

The comprehensive assessment of literature on cyber threat prediction using machine learning (ML) and deep learning (DL) approaches yielded substantial insights into the existing state-of-the-art, developing trends, and opportunities for future study. The main conclusions drawn from the research that have been analyzed are summarized in this section.

The initial phase in the evaluation process was locating pertinent publications that covered the application of deep learning (DL) and machine learning (ML) techniques for cyber threat prediction. A comprehensive search of electronic databases along with a manual analysis of reference lists yielded a total of 120 publications. This research covered a broad spectrum of cyber threat scenarios, including network intrusion detection, anomaly detection, and virus identification.

To guarantee excellent quality and relevance to the study topic, strict criteria were followed throughout the screening and selection of the articles. Following a comprehensive analytical process, eighty papers were chosen for additional investigation. This research addressed a wide range of cyber threat scenarios, including as denial-of-service (DoS) assaults, phishing scams and malware detection [22]. Furthermore, the chosen articles demonstrated the range of methods in the area by utilizing a variety of deep learning and machine learning techniques, including convolutional neural networks (CNN), recurrent neural networks (RNN), and support vector machines (SVM).

Data Extraction and Synthesis: A thorough picture of the development of the subject is produced by extracting and synthesizing data from a few chosen research on the improvements of machine learning (ML) and deep

learning (DL) techniques in cybersecurity. This systematic methodology allows for the identification of recurrent themes, developing patterns, and places where the investigations agree or disagree. Moreover, identifying fundamental concepts and insights is made possible by thematically synthesizing the gathered material.

Quality Assessment: Differences in sample size, data quality, methodological rigor, and reporting transparency were found in the evaluated research. Some research showed limitations due to limited sample numbers, lack of validation, or inadequate reporting information, while others showed resilience in experimental design and data processing. Overall, the quality evaluation gave significant insights into the strengths and limits of the existing literature on cyber threat prediction.

Data Analysis and Interpretation: To get important insights into the efficiency, applicability, and constraints of ML and DL algorithms in cyber threat prediction, the combined data were submitted to qualitative and quantitative analysis. Performance differences were found between several ML/DL algorithms, datasets, and assessment criteria through comparative analysis. While some techniques showed excellent accuracy and resilience in identifying known cyberthreats, major barriers to making trustworthy predictions in practical set- tings were class imbalance, data scarcity, and adversarial assaults.

Ethical Considerations: During the review process, ethical issues pertaining to informed consent, data privacy, and confidentiality were fully acknowledged and considered. Several precautions were taken to guarantee the ethical conduct of the research, such as following the ethical rules regulating academic research and properly attributing sources. Plagiarism was also avoided. Fig.2 compares the effectiveness of deep learning (DL) and machine learning (ML) models in identifying cyberattacks over time. It shows a steady pattern in which DL constantly outperforms ML in cyber threat detection. The study and analysis's conclusions confirm that deep learning is more predictive than machine learning, even if it does not explicitly show exact numerical values. The discovery that DL constantly outperforms ML in terms of detection rates during the whole timeframe under consideration leads to this conclusion. These revelations emphasize how dynamic cyber threat detection is and how crucial it is to use advanced analytics to strengthen cybersecurity resilience.

To sum up, the systematic review's findings offer insightful information on the state of cyber threat prediction today, utilizing ML and DL methods. Class imbalance, adversarial assaults, and data scarcity continue to be major difficulties despite advances in algorithmic sophistication and predictive modeling. To improve cybersecurity resilience in an increasingly digital environment and develop the area of cyber threat prediction, addressing these issues calls for multidisciplinary collaboration, methodological innovation, and ethical concerns.

V. Discussion

The discussion part explores the implications, constraints, and potential avenues for future research resulting from the integration of existing literature on machine learning (ML) and deep learning (DL) approaches for cyber threat prediction.

A. Implication Of Findings

Numerous implications for cybersecurity research and practice were found by the systematic study. First off, the efficacy of machine learning and deep learning techniques in cyber threat forecasting emphasizes how crucial it is to use sophisticated analytics to improve detection skills and counter new attacks. With the use of ML/DL models, it is possible to evaluate enormous volumes of heterogeneous data and spot minute trends that point to cyberattacks, allowing for prompt incident reaction and preventative protection measures.

The variety of ML/DL algorithms and approaches that have been studied in the literature also emphasizes the necessity for customized solutions that consider the particulars of various cyber threat situations. Recurrent neural networks (RNNs) [5] could be more suited for identifying temporal connections in sequential data streams, but convolutional neural networks (CNNs) [4] are excellent for evaluating network traffic data for intrusion detection. It is essential to comprehend the advantages and disadvantages of any strategy while creating successful cyber protection plans.

B. Limitation And Challenges

Though ML and DL have great potential for predicting cyber threats, there are still a number of obstacles and restrictions. First of all, a major barrier to the creation of precise and trustworthy prediction models is the lack of labeled training data. To properly train ML/DL algorithms, annotated datasets that represent the diversity and dynamism of real-world cyber threats are crucial. To ensure the resilience and generalization of prediction models, additional obstacles such as class imbalance, data quality concerns, and idea drift need to be tackled. Predictive modeling also has inherent uncertainties and weaknesses due to the adversarial nature of cyberattacks. Adversarial

assaults, such evasion and poisoning attacks, can alter input data to make ML/DL models less successful in practical situations by avoiding discovery. Sturdiness and resistance to hostile assaults are important fields of study to improve the dependability and credibility of cyber threat detection systems [23]..

C. Future Direction

The review of the literature on cyber threat prediction points to a number of directions for future investigation. First and foremost, to create comprehensive and context-aware methods for threat detection, multidisciplinary cooperation between cybersecurity professionals, data scientists, and domain specialists is required. Cybersecurity experts may make better decisions by combining domain expertise with ML/DL approaches to improve the predictability and explainability of predictive models. Additionally, the inherent uncertainties and antagonistic problems in cyber threat prediction should be the main focus of research efforts. ML/DL models may be made more resilient to adversarial attacks by utilizing strategies like ensemble learning, robust optimization, and adversarial training [24]. Additionally, the creation of standard assessment measures and benchmark datasets might help with repeatability and comparative analysis in cyber threat prediction research. In conclusion, the synthesis of literature on cyber threat prediction using ML and DL techniques provides valuable insights into the current landscape, challenges, and opportunities in cybersecurity. By addressing limitations, fostering interdisciplinary collaboration, and embracing innovative approaches, researchers can advance the state-of-the-art in cyber threat prediction and contribute to the resilience of digital ecosystems against evolving cyber threats.

VI. Conclusion

The assessment of the literature on machine learning (ML) and deep learning (DL) techniques for cyber threat prediction emphasizes how important advanced analytics are to fortifying cybersecurity defenses against dynamic attacks. Through a thorough analysis of research papers, this study provides significant insights into the state-of-the-art, issues, and future perspectives in cyber threat prediction. By using methods like convolutional neural networks (CNNs), recurrent neural networks (RNNs), and graph neural networks (GNNs) to analyze a variety of data sources and find patterns suggestive of cyberattacks, ML and DL ap- proaches provide promising paths for proactive threat detection and mitigation. However, there are several barriers to the creation of trustworthy and accurate prediction models, including issues with data scarcity, class disparity, and adversarial assaults. In spite of these obstacles, an analysis of the literature has shown a number of implications and chances for developing the subject of cyber threat prediction. The improvement of predictive modeling's efficacy and reliability depends critically on interdisciplinary cooperation, innovative methodology, and ethical issues. Through the integration of domain knowledge, the resolution of data quality concerns, and the adoption of resilient strategies against adversarial assaults, researchers can enhance the ability of digital ecosystems to withstand rising cyber threats. To sum up, cyber threat prediction is still a dynamic and developing industry that needs constant innovation and adaptation to keep one step ahead of competitors. In an increasingly linked world, cybersecurity professionals, academics, and policymakers may collaborate to improve the security and resilience of digital infrastructure by utilizing the insights and suggestions presented in this article.

References

[1] K Muthamil Sudar, P Deepa Lakshmi, P Nagaraj, and V Muneeswaran. Analysis of cyberattacks and its detection mechanisms. In 2020 Fifth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), pages 12–16. IEEE, 2020.

[2] Issa Qabajeh, Fadi Thabtah, and Francisco Chiclana. A recent review of conventional vs. automated cybersecurity anti-phishing techniques. Com- puter Science Review, 29:44–55, 2018.

[3] Arvid Kok, Ivana Ilic Mestric, Giavid Valiyev, and Michael Street. Cy- ber threat prediction with machine learning. Information & Security, 47(2):203–220, 2020.

[4] Wei Wang, Ming Zhu, Xuewen Zeng, Xiaozhou Ye, and Yiqiang Sheng. Malware traffic classification using convolutional neural network for repre- sentation learning. In 2017 International conference on information net- working (ICOIN), pages 712–717. IEEE, 2017.

[5] Keshava Srinivas, Narayanan Prasanth, Rahul Trivedi, Naman Bindra, and SP Raja. A novel machine learning inspired algorithm to predict real-time network intrusions. International Journal of Information Technology, 14(7):3471–3480, 2022.

[6] Asadi Srinivasulu and R Venkateswaran. Enhancing cybersecurity through advanced threat detection: A deep learning approach with cnn for pre- dictive analysis of ai-driven cybersecurity data. Journal of Research in Engineering and Computer Sciences, 1(5):65–77, 2023.

[7] Nuno Dion´ısio, Fernando Alves, Pedro M Ferreira, and Alysson Bessani. Cyberthreat detection from twitter using deep neural networks. In 2019 in- ternational joint conference on neural networks (IJCNN), pages 1–8. IEEE, 2019.
[8] Benjamin J Radford, Leonardo M Apolonio, Antonio J Trias, and Jim A Simpson. Network traffic anomaly detection using recurrent neural net- works. arXiv preprint arXiv:1803.10769, 2018.
[9] Md Raihan-Al-Masud and Hossen Asiful Mustafa. Network intrusion de- tection system using voting ensemble machine learning. In 2019 IEEE International Conference on Telecommunications and Photonics (ICTP), pages 1–4. IEEE, 2019.
[10] Kamran Shaukat, Suhuai Luo, Shan Chen, and Dongxi Liu. Cyber threat detection using machine learning techniques: A performance evaluation perspective. In 2020 international conference on cyber warfare and security (ICCWS), pages 1–6. IEEE, 2020.
[11] Abel Yeboah-Ofori, Shareeful Islam, Sin Wee Lee, Zia Ush Shamszaman, Khan Muhammad, Meteb Altaf, and Mabrook S Al-Rakhami. Cyber threat predictive analytics for improving cyber supply chain security. IEEE Ac- cess, 9:94318–94337, 2021.
[12] Mohit Sewak, Sanjay K Sahay, and Hemant Rathore. Deep reinforcement learning in the advanced cybersecurity threat detection and protection. Information Systems Frontiers, 25(2):589–611, 2023.
[13] Haoyu He, Yuede Ji, and H Howie Huang. Illuminati: Towards explaining graph neural networks for cybersecurity analysis. In 2022 IEEE 7th Euro- pean Symposium on Security and Privacy (EuroS&P), pages 74–89. IEEE, 2022.
[14] Omar Azib Alkhudaydi, Moez Krichen, and Ans D Alghamdi. A deep learning methodology for predicting cybersecurity attacks on the internet of things. Information, 14(10):550, 2023.
[15] Stefano Silvestri, Shareeful Islam, Spyridon Papastergiou, Christos Tza- gkarakis, and Mario Ciampi. A machine learning approach for the nlp-based analysis of cyber threats and vulnerabilities of the healthcare ecosystem. Sensors, 23(2):651, 2023.
[16] Anjali Rajak and Rakesh Tripathi. Dl-sklstm approach for cyber security threats detection in 5g enabled iiot. International Journal of Information Technology, 16(1):13–20, 2024.
[17] Ebuka Chinaechetam Nkoro, Cosmas Ifeanyi Nwakanma, Jae-Min Lee, and Dong-Seong Kim. Detecting cyberthreats in metaverse learning platforms using an explainable dnn. Internet of Things, 25:101046, 2024.
[18] Prabhat Kumar, Danish Javeed, Randhir Kumar, and AKM Najmul Islam. Blockchain and explainable ai for enhanced decision making in cyber threat detection. Software: Practice and Experience, 2024.
[19] Andrew Booth. Searching for qualitative research for inclusion in system- atic reviews: a structured methodological review. Systematic reviews, 5:1– 23, 2016.
[20] Ant´onio Pedro Costa and Maria Cec´ılia de Souza Minayo. Building criteria to evaluate qualitative research papers: a tool for peer reviewers. Revista da Escola de Enfermagem da USP, 53:e03448, 2019.
[21] Eli Lieber. Mixing qualitative and quantitative methods: Insights into design and analysis issues. Journal of Ethnographic & Qualitative Research, 3(4), 2009.
[22] A Babate, M Musa, A Kida, and M Saidu. State of cyber security: emerg- ing threats landscape. International Journal of Advanced Research in Com- puter Science & Technology, 3(1):113–119, 2015.
[23] Muhammed Zekeriya Gunduz and Resul Das. Cyber-security on smart grid: Threats and potential solutions. Computer networks, 169:107094, 2020.
[24] Afnan Alotaibi and Murad A Rassam. Adversarial machine learning attacks against intrusion detection systems: A survey on strategies and defense. Future Internet, 15(2):62, 2023