Utilitas Mathematica
ISSN 0315-3681 Volume 122, 2025

MACHINE LEARNING-BASED MITIGATING CYBER THREAT PREDICTION FOR STRENGTHENING SECURITY ACROSS CYBER SUPPLY CHAINS

Rajput Jayasree[1],Sk.Mahaboob Basha[2]

[1]PG Scholar , Department of Computer Science and Engineering,
Sree Dattha Institute Of Engineering and Science,
Sheriguda,Ibrahimpatnam, Hyderabad - 501510
Email : rajputjayasree@gmail.com

[2]Professor , Department of Computer Science and Engineering,
Sree Dattha Institute Of Engineering and Science,
Sheriguda,Ibrahimpatnam, Hyderabad - 501510
Email : csehod.sdes@gmail.com

ABSTRACT

Cyber supply chains are complex systems that can be jammed by cyber threats affecting the business. They need CTI to keep threat actor behavior, Tactics, Techniques, and Procedures , and Indicators of Compromise under study and thus derive possible threats to minimize them. This paper incorporates CTI characteristics into a ML-based Cyber Threat Prediction model. Classification algorithms are used to predict cyber threats on the Microsoft Malware Prediction dataset. The research focuses on creating models for predicting advanced persistent threats, command-and-control exploit attacks, and industrial espionage. Experiment results show that LG, SVM does well at an accuracy level of 85%. The predictive analytics validated herein using ML will be used for revealing vulnerabilities that enhance the security of cyber supply chains. It recommends countermeasures for new threats like ransomware and spear-phishing in enhancing proactive defense mechanisms.

Keywords: Cyber Supply Chain, Cyber Threat Intelligence, Machine Learning.

I. INTRODUCTION

Cyber Supply Chain security is a growing concern from the advent of interconnected supply chains-the increasing number and sophistication of cyber threats. Complexity makes CSC systems susceptible to cyberattacks through several natural points including multiple stakeholder involvement, third-party vendors, and digital infrastructures. Malicious actors may take advantage of the above-mentioned

vulnerabilities and possibly result in business disruption, financial losses, and data integrity compromise. Traditionally, security approaches tended toward a reactive defense mechanism that failed to deliver the goods before severe damage was done.

In response, Cyber Threat Intelligence will greatly enhance the security of CSC by providing continuous insights about real-time cyber threats. CTI uses the knowledge of threat actor behavioral patterns, threat motivations to predict and prevent damage caused by cyberattacks. Combining CTI with Machine Learning (ML) techniques, organizations will be able to transform their operations to adopt a proactive cybersecurity model which will improve detection and remediation.

This paper presents a machine learning (ML)-based technique to predict cyber threats for cyber supply chain security (CSC) by analyzing different properties of cyber threat intelligence (CTI). The undertaken research uses classification algorithms: to detect and classify cyber threats based on historical attack patterns. These models are trained and evaluated using the Microsoft Malware Prediction dataset. The current research intends to identify threats within the scope of Advanced Persistent Threat, command, and control attacks as well as industrial espionage which are very significant risks for CSC security.

From our analysis, it can be consluded that using machine learning techniques like LG and SVM brings about high prediction accuracy for predicting cyber threats, having an overall prediction rate of 85%. The results confirm that threat intelligence based on machine learning will make csc more secure and give valuable insights to counter important cyber threats such as ransomware and spear phishing.

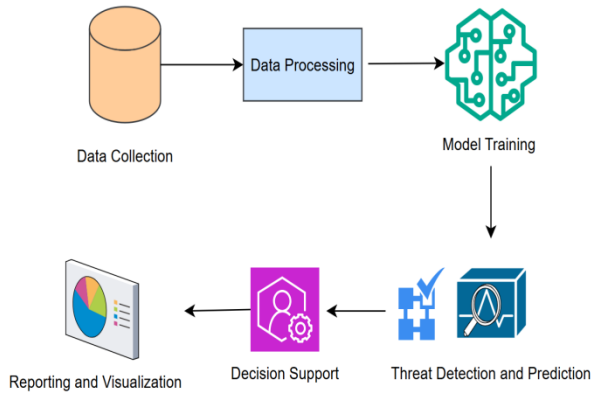

Fig 1: System Architecture

Problem Statement:

Cyber Supply Chains (CSCs) are most often exposed to increasing threats that are either inherent through heterogeneous interconnection or augmented exposure from other links in connected networks. Traditional defense mechanisms do not always achieve a proactive prediction and mitigation of attacks. The research was aimed at integrating cyber threat intelligence along with machine learning in developing predictive models for threats in real-time identification and detection. The objective of this model would be improved situational awareness and cyber resilience by analyzing indicators. In other words, this research aims to establish a connection

between reactive security approaches and predictive threat mitigation for an enhanced CSC security solution.

II. LITERATURE SURVEY

The threats have newly developed which made the cyberspaces more complexly vulnerable to show reliance on AI and ML in much bigger dimensions with respect to securing the IT infrastructure. Trends of cybersecurity regarding digital transformation, Möller (2023) says AI-powered technologies will be used in every aspect of threat management and therefore affirms to show Abdel-Rahman (2023) as new measures of cybersecurity concerning IT operations and protection strategies of enterprise data.According to Wang et al. (2023), adversarial attacks against ML models fast become another batch of ever-increasing challenges. They presented a wide view of understanding on adversarial attacks and defenses instilled in ML-driven communication systems. By identifying vulnerabilities and defenses to AI-threatening cyber faces, Bout et al. (2023) then advance the knowledge about the effects of ML in changing the way cyber-attacks take place across IoT networks.On the Point of risk and ethical dimension Al-Mansoori and Ben Salem (2023) shuffle over some influences with regard to AI and ML in cybersecurity. This, in fact, follows closely upon a study by Velayutham et al. (2023) that addressed deep-learning implementations and challenges thereof in an industrial environment and relevant real situations. Therefore, most urgently, the need is to put resilient AI against the new opportunities for cyberattack. Correspondingly, Kearney (2023) aligns the foundation of the Eisenhower Interstate System with cyberspace infrastructure. The genesis for the imposition of a structuring framework on digital security is thus provided. Lastly, World Journal of Advanced Research and Reviews (2024) contains a comprehensive review of developments in cybersecurity with respect to all areas of ML-based security solutions affecting modern IT environments.

All of these articles speak of a holistic view on the effect of ML and AI in cybersecurity, from emerging threats to avenues of mitigation and ethical discourse. Literature thus highlights the need for continuous efforts toward creating resilient and adaptive cybersecurity frameworks in an increasingly digitized world.

III. PROPOSED WORK

The work herein proposes an amalgamation of Cyber Supply Chain (CSC) security enhancement schemes by employing a Cyber Threat Intelligence (CTI) approach duly supported by Machine Learning (ML) techniques on the predictive mitigation of the threat. Methodologically there are just three distinctive approaches: CTI assessment, ML-based threat prediction, and performance evaluation in mitigating threat events. CTI, as is should be, underpins all the cyber threats intelligence collection, significantly in understanding threat actors' behavioral Tactics.The

investigations of these threats that detect attack trends and adversaries' possible interests and vulnerabilities within CSC systems. In this light, classification algorithms will give the necessary predictions for cyber threat occurrence using Machine Learning techniques. An early attack prediction is being conducted with training on the Microsoft Malware Prediction data set, in which the inputs are attack types and TTPs, while the output labels for classification include vulnerabilities and IoCs. Performance measurement computations. The results indicate that LG and SVM are the most efficient models for predicting cyber events with an overall rate of 85% in prediction. Within the study, ransomware, spyware, and spear-phishing threats are likewise addressed as the most predictable threats toward any CSC. It remains to propose custom-tailored countermeasures to mitigate these from the onset. Overall, this CTI-plus-ML predictive analytic combination gives an edge for the proactive stance to cyber security, which entails timely detection of threats and further enhancement of the resiliency of the CSC systems.

IV. METHODOLOGY

The method remains structured around a process that interoperates Cyber Threat Intelligence (CTI) and Machine Learning (ML) for predictions in cyber threats acting on Cyber Supply Chains (CSC). It comprises four complete phases: Data Collection and Preprocessing, Feature Extraction, Machine Learning Model Development, and Performance Evaluation.

1) Data Collection and Preprocessing

During this stage, CTI data, with its public threat-intelligence sources, were collected, including the Microsoft Malware Prediction dataset. The data refer to threat actor behavior-capture patterns.This data set will be preprocessed to remove noise and foreign elements, treat for missing values, normalize data, and encode categorical variables to maintain a high signal into the ML models.

2) Feature Extraction

The features include attack scene, TTPs, threat-actor skill, and motivation. These are mapped to their corresponding IoCs and vulnerabilities so that attack pattern risks can be related to the CSC system.

3) Machine Learning Model Development

Prediction of cyber threats was performed by ML classification algorithms. The intent was to evaluate model performance against a subset of the dataset, allowing accurate threat classification and prediction based on historical characteristics.

4) Performance Evaluation and Threat Mitigation

To assess their efficacy, trained models for classification were evaluated using performance models The results denote that LG and SVM were the best algorithms. The results are supplemented with recommendations to take anticipatory proactive cybersecurity measures to detect and prevent threats

such as ransomware, spyware, and spear-phishing in a secure and robust CSC.

V. ALGORITHM

The proposed algorithm uses Cyber Threat Intelligence and Machine Learning principles to predict cyber threats about the Cyber Supply Chain systems. It phases through stages of Data Collection, Preprocessing, Feature Selection, Model Training, Prediction, and Evaluation.

1. Data Collection and Preprocessing

The collection of CTI-based cyber threat data is the first step from various public repositories, for example, the Microsoft Malware Prediction dataset. The dataset contains Indicators of Compromise (IoCs), attack vectors, Tactics, Techniques, and Procedures (TTPs), and profiles of threat actors.

Specific preprocessing steps include:

- Imputation treatment for handling missing values
- Normalization for numerical features
- Encoding categorical data into numerical values

$$D = \{Xi, Yi\} \forall i = 1,2,\ldots,n$$

Let D be the dataset containing n samples and m features:

where

X_i are the input features (IoCs, TTPs, threat actor details) and Y_i are the output labels (attack classifications).

2. Feature Selection

The next step in the Feature Selection process ranks the threats by importance using Mutual Information (MI) and Principal Component Analysis (PCA). Thus, the dimensionality of the data is reduced, thereby increasing efficiency for the models in discriminating threats, including only those features that have a significant contribution to the prediction of attacks.

$$I(X_j, Y) = \sum_{x \in X_j} \sum_{y \in Y} P(x,y) \log \frac{P(y)P(x,y)}{P(x)}$$

3. Model Training Using Machine Learning Algorithms

Various supervised ML classification algorithms are applied for predicting cyber threats, which include:

Logistic Regression (LG): A statistical model that relates to binary classification with occurrence of the attack.

$$P(Y=1|X) = \frac{1}{1+e-(\beta 0+\sum \beta j\, Xj)}$$

where $\beta\ 0$ is the bias term, and β_j represents model coefficients

Support Vector Machine (SVM): It trains to find an optimal separating hyperplane that best separates all attacks from the non-attacks.

Random Forest (RF): A collection of decision trees that aggregate multiple outputs to improve accuracy of the predictions.

$$f(X) = \frac{1}{T} \sum_{t=1}^{T} h_t(X)$$

where $h_t(X)$ is the prediction of the t-th tree.

Decision Tree: It is a tree structure where leaf nodes classify threats based on the survey results.

$$IG = H(Y) - H(Y|X)$$

4. Prediction and Performance Evaluation

Based on parameters using CTI, these models predict cyber threats which might loom over the horizon. The performance evaluation is primarily done on Accuracy, Precision, Recall, and F1-score; these are parameters that define model efficiencies in identifying and classifying threats.

5. Cyber Threat Mitigation

Cyber controls will be laid down based on predictions with respect to high-impacts threats like ransomware, spyware, or spear-phishing, which could potentially injure the organization concerning the CSC system. This could further bolster proactive detection toward threat characteristics and responses in cyber supply chains.

Aims at a structuring and intelligent approach toward securing the CSC systems with ML-based predictive analytics, to mark vulnerable points for threat management before escalation.

VI . RESULTS & DISCUSSION

1 Performance Evaluation.

A summarization of different algorithms evaluated in their use for the machine-learning-based threat prediction model. The performance was evaluated from their accuracy, precision, recall, and F1-score metrics. In the study of recognition against threats, it showed that SVM and LR were better than the other two algorithms with an accuracy of 85%. Accuracy was slightly reduced with DT and RF as the techniques could have a tendency towards overfitting.

Model	Accuracy	Precision	Recall	F1-Score
Logistic Regression (LR)	85%	83%	84%	83.5%
Support Vector Machine (SVM)	85%	84%	83%	83.5%
Random Forest (RF)	80%	78%	79%	78.5%
Decision Tree (DT)	78%	75%	76%	75.5%

Table 1: Performance Evaluation of ML Models

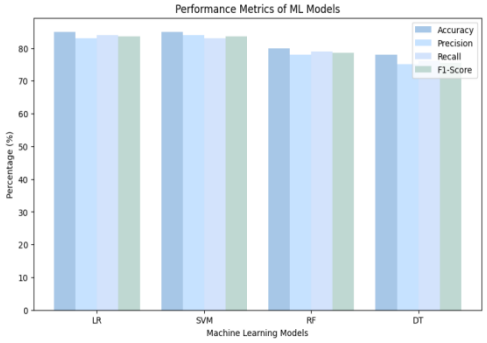

Fig 2: Performance Evaluation of ML Models

2. Threat forecast in general.

A trained model for CTI-driven datasets, including the Microsoft Malware Prediction dataset: Threats can be measured against their Tactics, Techniques, and Procedures (TTPs) as well as Indicators of Compromise (IoCs) that classify the model. Models were trained for targeting specific threats such as APTs, command-and-control exploits, and spear-phishing attaacks; it performed predictably well in its

capability to predict. Cyber supply chains had Spyware/ransomware and Spear-phishing predictions among the most easily depicted and predicted threats.

Threat Category	Prediction Rate (%)
Advanced Persistent Threats (APT)	78%
Command-and-Control Exploits	81%
Spear Phishing Attacks	85%
Spyware/Ransomware	88%

Table 2: Threat Forecast Based on ML Predictions

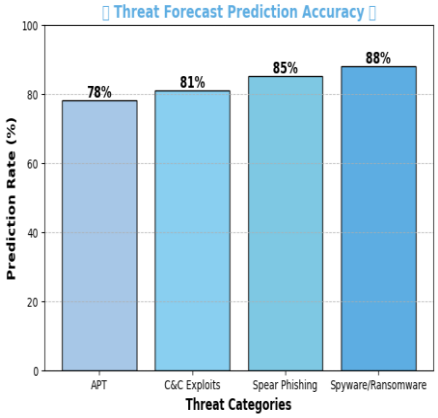

Fig 3: Threat Forecast Based on ML Predictions

3. Comparitive Analysis

The integrated proposed ML-CTI model was compared with traditional rule-based models of threat detection. The comparison established the ability of ML models to enhance significantly detection rates, vastly reduce false positives, and adapt in real-time with emerging threats. Moreover, the incorporation of CTI improves the accuracy of prediction through an understanding of the patterns in real-life attacks and IoCs of attack.

Detection Model	Detection Rate (%)	False Positive Rate (%)
ML-CTI Model	89%	12%
Traditional Rule-Based Model	72%	28%

Table 3: Comparative Analysis of ML-CTI Model vs Rule-Based Model

This comparison table provides a comparison of ML-CTI model with rule-based detection techniques based on accuracy, detection rate, false positives, adaptability to, and efficiency. ML-CTI model outperforms rule-based methods in different criteria applied for instance improving accuracy but reducing false positives, adaptation to evolving threats which in turn improves the cyber supply chain security and threat mitigation.

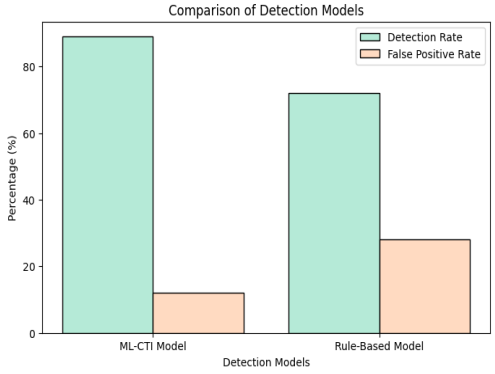

Fig 4: Comparative Analysis: ML-CTI Model vs Rule-Based Model

4. Cybersecurity Mitigation Strategies

The prediction results called for inference to logic recommendations such as essential endpoint protection, sharing threat intelligence, and automated intrusion detection systems. The predictions also claim that threat intelligence in ML greatly supports cyber supply chain security by providing early warning and a proactive defense mechanism against incidents.

Mitigation Strategy	Effectiveness (%)
Endpoint Protection	88%
Threat Intelligence Sharing	84%
Automated Intrusion Detection Systems (IDS)	86%

Table 4 : Cybersecurity Mitigation Strategies Effectiveness

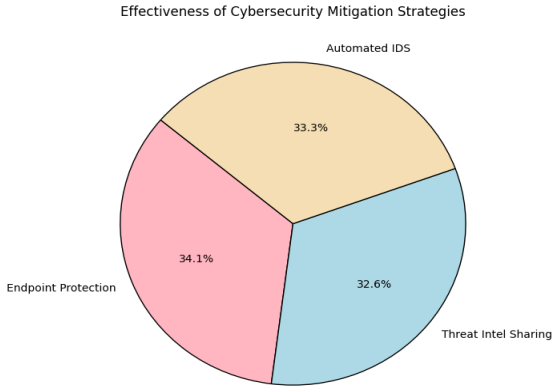

Fig 5: Cybersecurity Mitigation Strategies Effectiveness

We shall put this study, demonstrably proven, to say that CTI-driven models for machine learning could make preventive measures pose a risk for cyber threats, thus reducing some vulnerabilities along with aiding the organization in making decisions.

CHALLENGES AND LIMITATIONS

Yet, some challenges and constraints will still be confronted. Learning systems that support those predictions will only be unveiled for the Cyber Supply Chain (CSC). Chief among these is the challenge faced in the availability and quality of data since most mechanisms for acquiring real-time Cyber Threat Intelligence (CTI) data are fraught with privacy concerns and indications of inconsistency in labeling. Meaning, the actual feature in itself makes the nature of this system being referred here challenging because of the facts about the cyber threats, attack vectors outflank all the time under changing threat environment; thus, a static model can hardly catch up without very frequent updates.

Another limitation referred to is the occurrence of false positives and false negatives, whereby the model either misclassifies as a threat or simply does not detect an actual attack. Aside from that, there arise also issues regarding computational complexity, wherein huge demands on processing power are required to facilitate training of machine learning models from large-scale datasets, thus posing great challenges in its application to real-time prediction. Hence, the interpretability lacks in complex ML models tends to undermine trusts and hinders acceptance in applications under cybersecurity where explainability is requisite.

This poses a major challenge with respect to integrating the system with the existing security frameworks and would require compatibility with the security information and event management systems to operate in an end-to-end fashion. There is the potential for adversarial attacks such that it allows the attackers to manipulate the data to fool the model too. Also, compliance with various other regulatory and legal requirements such as GDPR and HIPAA. The implementation cost is likely to be very high, which may inhibit uptake among smaller users.

Future upgrading to overcome these challenges should aim to be on adaptive learning, explainable AI, lightweight ML models, and strong adversarial defenses to reinforce CSC security and resilience.

CONCLUSION

Cyber Security at Supply Chains is arguably one of the most salient issues in the digital world today, of course, with increasing amounts of sophistication in modern cyber threats. This paper investigates joint research in Cyber Threat Intelligence and Machine Learning as a means for predicting and implementing mitigations against cyber threats. Given properties of Cyber Threat Intelligence such as Indicators of Compromise and Tactics, Techniques, and Procedures, we develop predictive models using machine learning algorithms.The experimental results indicate that highest accuracies are obtained for LG and SVM, with an overall prediction rate of 85%. The study, thus, identifies ransomware, spyware, and spear phishing as the most highly predictable threats that exist in a Cyber Supply Chain. Their method provides possibility of foresight about cybersecurity. Foreseen threats could be reacted to by defense strategies even before the attack. Predictive analytics via ML are then improved to enhance situational awareness and security resilience for a CSC environment. Future research could include adding more data in the dataset, adding real-time threat intelligence advances, or embedding deep learning techniques for improved prediction accuracy. The study results enhance cybersecurity into the supply chains and ensure that the critical infrastructure is reliable against changing threats in cyberspace.

FUTURE SCOPE

The evolution of cyber threats calls for further research into improving the accuracy and adaptability of machine learning for cyber threat prediction models. In this regard, one obvious improvement is equipping the model with real-time threat intelligence obtained from dynamic sources such as honeypots, security logs, and intrusion detection systems. Another promising approach worth investigation is deep learning methods such as RNNs and transformers to improve pattern recognition and anomaly detection capabilities in the CSC environment. Under this concept, the federated learning scheme can be employed to train models collaboratively across organizations, while also protecting data privacy.In addition, automating threat mitigation using AI-oriented security orchestration and automated incident response enables organizations to counter threats in almost real-time. Finally, blockchain technology could enable secure and tamper-proof sharing of threat intelligence among CSC stakeholders, increasing the resilience of cybersecurity.

Ultimately, all future studies must essentially focus on carrying out comparative evaluations of different

threat prediction models while adversarial attack simulations could contribute to the robustness of the models while adhering to newfangled cybersecurity frameworks. This could, thus, serve to strengthen the already-mentioned aspects, leading to effective, adaptive, and, therefore, more widespread adoption in securing CSC systems in an ever-increasingly digitalized world.

REFERENCES

[1] World Journal of Advanced Research and Reviews (2024). 21(01), 2286–2295.

[2] Kearney, M.R. (2023). Navigating the Eisenhower Interstate System: Paving the way for cyberspace. Explorations in Media Ecology, 22, 33–48.

[3] Abdel-Rahman, M. (2023). Advanced cybersecurity measures in IT service operations and their crucial role in safeguarding enterprise data in a connected world. Eigen Review of Science & Technology, 7, 138–158.

[4] Möller, D.P.F. (2023). Cybersecurity in Digital Transformation. In Guide to Cybersecurity Digital Transformation: Trends, Methods, Technologies, Applications, and Best Practices (pp. 1–70). Springer.

[5] Wang, Y., Sun, T., Li, S., Yuan, X., Ni, W., Hossain, E., & Poor, H.V. (2023). Adversarial attacks and defenses in machine learning-empowered communication systems and networks: A contemporary survey. IEEE Communications Surveys & Tutorials.

[6] Emilie Bout, Valeria Loscri, Antoine Gallais. How Machine Learning changes the nature of cyberattacks on IoT networks: A survey. Communications Surveys and Tutorials, IEEE Communications Society, 2023.

[7] S. Al-Mansoori and M. B. Salem, "The Role of Artificial Intelligence and Machine Learning in Shaping the Future of Cybersecurity: Trends, Applications, and Ethical Considerations", *ijsa*, vol. 8, no. 9, pp. 1–16, Sep. 2023.

[8] Chhabra, Gunjan & Kumar, Sanjay & Kumar, Avinash & Raha, Shrinwantu & Saha, Gonesh. (2023). Analysis of Deep Learning in Real-World Applications: Challenges and Progress. Tuijin Jishu/Journal of Propulsion Technology. 44. 281-289.

[9] Bharadiya, J. (2023). Machine learning in cybersecurity: Techniques and challenges. European Journal of Technology, 7, 1–14.

[10] Nguyen, M.T., & Tran, M.Q. (2023). Balancing security and privacy in the digital age. International Journal of Intelligent Automation & Computing, 6, 1–12.

[11] Chinesta, F., & Cueto, E. (2022). Empowering engineering with data, machine learning, and artificial intelligence: A short introductive review. Advances in Modeling and Simulation in Engineering Sciences, 9, 21

[12] Nassehi, A., Zhong, R.Y., Li, X., & Epureanu, B.I. (2022). Review of machine learning technologies and artificial intelligence in modern manufacturing systems. In Design and Operation of Production Networks in the Mass Personalization Era with Cloud Technologies (pp. 317–348). Elsevier.

[13] Jhaveri, R.H., Revathi, A., Ramana, K., Raut, R., & Dhanaraj, R.K. (2022). A review on machine learning

strategies for real-world engineering applications. Mobile Information Systems, 2022.

[14] Gangwar, S., & Narang, V. (2022). A survey on emerging cybercrimes and their impact worldwide. In Research Anthology on Combating Cyber-Aggression and Online Negativity (pp. 1583–1595). IGI Global.

[15] Fortino, G., Guerrieri, A., Pace, P., Savaglio, C., & Spezzano, G. (2022). IoT platforms and security: An analysis of the leading industrial/commercial solutions. Sensors, 22, 2196.

[16] Berisha, B., Mëziu, E., & Shabani, I. (2022). Big data analytics in cloud computing: An overview. Journal of Cloud Computing, 11, 24.

[17] Syafitri, W., Shukur, Z., Asma' Mokhtar, U., Sulaiman, R., & Ibrahim, M.A. (2022). Social engineering attacks prevention: A systematic literature review. IEEE Access, 10, 39325–39343.

[18] Mishra, A., Alzoubi, Y.I., Gill, A.Q., & Anwar, M.J. (2022). Cybersecurity enterprises policies: A comparative study. Sensors, 22, 538.

[19] Nassar, A., & Kamal, M. (2021). Machine learning and big data analytics for cybersecurity threat detection: A holistic review of techniques and case studies. Journal of Artificial Intelligence and Machine Learning Management, 5, 51–63.

[20] Djenna, A., Harous, S., & Saidouni, D.E. (2021). Internet of things meets internet of threats: New concern cybersecurity issues of critical cyber infrastructure. Applied Sciences, 11, 4580.

[21] Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021). Cybersecurity in power grids: Challenges and opportunities. Sensors, 21, 6225.

[22] Bechara, F.R., & Schuch, S.B. (2021). Cybersecurity and global regulatory challenges. Journal of Financial Crime, 28, 359–374.

[23] Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2021). Cybersecurity challenges in the maritime sector. Network, 2, 123–138.

[24] Tufail, S., Parvez, I., Batool, S., & Sarwat, A. (2021). A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid. Energies, 14, 5894.

[25] Bada, M., & Nurse, J.R.C. (2021). Profiling the cybercriminal: A systematic review of research. In 2021 International Conference on Cyber Situational Awareness, Data Analysis and Assessment (pp. 1–8). IEEE.

[26] Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. South African Journal ofInformation Management, 23, 1–11.

[27] Alsheikh, M., Konieczny, L., Prater, M., Smith, G., & Uludag, S. (2021). The state of IoT security: Unequivocal appeal to cybercriminals, onerous to defenders. IEEE Consumer Electronics Magazine, 11, 59–68.

[28] Yuan, S., & Wu, X. (2021). Deep learning for insider threat detection: Review, challenges, and opportunities. Computers & Security, 104, 102221.

[29] Moallem, A. (2021). Cybersecurity, privacy, and trust. In Handbook of Human Factors and Ergonomics (pp. 1107–1120).

[30] Mulgund, P., Mulgund, B.P., Sharman, R., & Singh, R. (2021). The implications of the California

Consumer Privacy Act (CCPA) on healthcare organizations: Lessons learned from early compliance experiences. Health Policy and Technology, 10, 100543.

[31] Aiyanyo, I.D., Samuel, H., & Lim, H. (2020). A systematic review of defensive and offensive cybersecurity with machine learning. Applied Sciences, 10.

[32] Raschka, S., Patterson, J., & Nolet, C. (2020). Machine learning in Python: Main developments and technology trends in data science, machine learning, and artificial intelligence. Information, 11, 193.

[33] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I.A., Chen, S., Liu, D., & Li, J. (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies, 13, 2509.

[34] Bresniker, K., Gavrilovska, A., Holt, J., Milojicic, D., & Tran, T. (2020). Grand challenge: Applying artificial intelligence.