Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 3, 2026

THREAT INTELLIGENCE FOR CYBER ATTACK PREDICTION

Mazhar Ali[1], Faheem Ahmed[2], Kamran Dahri[3], Rida Sara Khan[4], Yaqoob Koondhar[*5]

[1,2,3]*Department of Information Technology, University of Sindh, Jamshoro*
[4]*Shaheed Zulfikar Ali Bhutto Institute of Science and Technology*
[*5]*Information Technology Centre, Sindh Agriculture University Tandojam*

[*1]mazhara94@yahoo.com, [2]faheem.abbasi@usindh.edu.pk, [3]kamran.dahri@usindh.edu.pk,
[4]rida.sara@hyd.szabist.edu.pk, [5]yaqoobkoondhar@sau.edu.pk

DOI: https://doi.org/10.5281/zenodo.19202395

Keywords

Article History
Received: 25 January 2026
Accepted: 08 March 2026
Published: 24 March 2026

Corresponding Author: *
Muhammad Yaqoob Koondhar[5]
yaqoobkoondhar@sau.edu.pk

Abstract

This respective research examined threat intelligence (TI) as the proactive ability to identify and respond to cyber threats and highlights machine learning as the means to bolster cybersecurity. As digital infrastructures increase so does the potential for risks such as ransomware DDoS APTs etc. In most cases, established approaches to cybersecurity fail at detecting such threats; thus, turning to a predictive model. In this paper, different machine learning algorithms such as neural networks, decision trees, random forest, and Support Vector Machine are discussed to enhance the threat detection process. Thus, Neural networks as far as accuracy are the best when it comes to identifying such special features which are crucial in identifying new kinds of threats. On the other hand, random forests offer a nice middle ground in terms of accuracy ensuring that there is explainable adherence to compliance requirements such as in the financial or health care sectors. The research also explores areas of specific interest regarding the applicability of TI within different sectors, and its effectiveness. The results emphasize one method for future enhancements in TI: improved data-sharing procedures, ethical artificial intelligence, and models that can endure novel threats. To the best of the author's knowledge, this study fills this gap through advancing the framework for a multi-layered TI approach and improving the advancement of organizations' capabilities to appropriately address cyber threats within a constantly evolving digital terrain.

INTRODUCTION

Over the last few years, the advance in internet and technological platforms has presented many prospects and smoother operations in all fields. While driving growth and diversification across digital platforms this growth increased the susceptibility of systems, networks and data to numerous cyber risks. Cyber threats continue to escalate, and at the same time, the complexity of ransomware, DDoS, and APT is increasing in various sectors of both the public and private domains. While they interfere with normal commercial processes, attacks can cause significant financial, image, and sometimes national losses (Zhao et al., 2021). In this regard, generic information security solutions have been found to lack effectiveness when it comes to fighting ever emerging threats; therefore, the emphasis has been placed on proactive and predictive solutions like TI.

Threat intelligence refers to the process of identifying the information on a threat or threats and processing, analyzing this information. Thus, this research focuses on the efficiency of TI in

identifying and evaluating threats before they occur to improve the organizations' protection. And no longer is it just about passively looking for existing openings, TI is proactive too where practitioners engage in the seeking of indicators of compromise, studying adversary tactics, technical and procedural (TTPs) and involves lookout for a range of data such as net logs, social media updates or even the dark web. Through such datasets, TI disseminates the information that cybersecurity specialists need to effectively respond to cyber threats before they happen. In the work of Rodriguez and Costa (2024), the authors note that TI doubles the effectiveness of security plans, allowing organizations to predict threats instead of reacting after the fact has happened.

At the heart of the TI's ability to forecast the attacks is the application of big data analysis, Artificial Intelligence (AI) and Machine Learning to identify nascent patterns which are suggestive of an imminent attack. This paper is concerned with these technologies' usage in the TI, wondering how algorithms can work through large data sets quickly to identify outliers suggesting an attack may be immanent. For example, machine learning is particularly used in identifying the abnormal behavior within the network traffic or activities executed by the users. These real time alerts, allow cyber defense teams to intervene quickly, which minimizes the potential damage of emergent threats (Alsaedi et al., 2022). In addition, machine learning in TI does not strictly concern with identifying anomalies, but also predictive models to aid organizations, detect threats that do not fall under the overall pattern, for example, zero-day attacks, which are the usual blind spots for traditional systems that operate based on statistical data (Kure et al., 2022).

The study also questions current cybersecurity models where more often than not these models fail to factor in new threats as they depend on the past incidences. This work showcases how with its predictive concentration, TI, changes the facet of cybersecurity from being residual to being prospective; a factor that is particularly crucial given the ever increasing integration of technology in today's world systems. Together with data analysis and data-based prediction, TI helps organizations increase their level of readiness for threats, identify threats that can pose a risk to their infrastructure, and respond to threats before they turn into a weak link for the organization (Georgiadou et al., 2023).

This paper also discuss the execution of TI in real life situations in the financial context, the health care industry and national defense. The research provides an insight as to how organizations in these fields employ threat intelligence systems in detecting, forecasting and mitigating prospective cyber threats cutting to the Chase the special predicaments facing their operations. For example, markers in TI are used in healthcare organizations to identify early signs of ransomware, and in financial organizations, to counter DDoS threats. These example show how important is TI to solve different cybersecurity issues and prove that it should be used to protect valuable data and information for important sectors (Weng & Wu, 2024).

Therefore, this work has demonstrated the appropriateness of threat intelligence in the modern world of security threats. In reviewing the methodologies, applications and benefits of TI on cyber-attack prediction, this paper offers a clear understanding of how predictive threat intelligence empowers organizations to combat the ever emerging threats. The current study underscores the need for TI system enhancement, enhancement in integration of AI into TI systems, data sharing, as well as addressing the ethical issues to address the modern world complexities and to offer proper security measures against modern day computerized threats.

Literature Review

The literature on threat intelligence tends to explain TI as a shift toward proactive cybersecurity measures based on the gathering, analysis, and interpretation of data on future threats. TI helps organizations to learn what TTPs the adversaries are likely to use in order to defend themselves. This section gives an overview of the noteworthy works in threat intelligence as represented in table 1 below which gives an overview of the key research contributions to TI models, frameworks and algorithms.

Overview of Threat Intelligence and Its Levels

Capgemini et al. (2021) discussed the initial work done to segregate TI into levels, which play different roles in cybersecurity frameworks. TI is generally divided into three levels: The level of planning can be broadly categorized into three; Tactical planning, operational planning, and strategic planning. Tactical threat intelligence deals with details including the category of threat as well as its manifest attributes like malware identifiers and IP numbers which enable the taking of actions against noted threats. On the other hand, operational threat intelligence delivers wider information concerning adversary TTPs that helps security teams gain more understanding about the behaviors of attackers and possible points of entrance. Strategic threat intelligence is on a macro level, identifying the adoptions of the threat actors in the progression of the threat situation to inform top-line planning and policy formulation (Sarker et al., 2021). Having identified that TI constitutes a conceptually complex area, the authors continue to present diverse layers, which collectively guarantee that organizations can tackle cybersecurity issues across the range of preventively, toward quickly fixing them, and prospectively.

Artificial Intelligence in Threat Intelligence

AlZubi et al. (2021) advance the knowledge by analyzing the changes of TI through the integration of AI. With the threat actors evolving to a level where they are unleashing bigger and even more complex attacks, conventional security models have been unable to cope. AlZubi et al. (2021) highlighted that with the help of such AI techniques as machine learning and natural language processing and deep learning, the TI systems can analyze the massive amount of diverse data within the area of interest. For instance, AI models can identify minor trends in social media and network traffic and other cybersecurity activities such as discussion in the dark web for which human analysts are capable of identifying in real-time. Moreover, the use of AI in TI can be to provide the means for predictive analysis so that any possible threats that might unfold in future can be detected enabling organizations to transition to pro-action instead of reacting to existing threats. The adoption of AI in conjunction with TI frameworks is a significant step in the current generation's cybersecurity given the AI's ability to help identify threats in organizations with vast data, such as finance and health, all before significant disruptions occur.

Machine Learning for Threat Detection

The essence of automation and optimization of threat detection at TI is ML, as discussed by Ben Fredj et al. (2020). This paper also examined the use of supervised and unsupervised learning approaches for detecting cyber threats using anomaly detection and pattern recognition techniques. Supervised learning models use data with known threats such as phishing emails, or known malware to classify known threats. These models are particularly useful in detecting novelties in a set of values concerning a given feature, for instance, login hours and data transmission rates that differ from the majority of other similar values. According to Ben Fredj et al. (2020), decision trees, support vector machines and k-means clustering used for the development of TI systems integrate capabilities allowing such systems to learn from the data accumulated and improve the parameters of detection, as well as their flexibility. These ML models have become a necessity for TI especially in RTCC applications including IoT where the standard security precaution methods are slow in processing and dealing with the ever increasing rate of data transfer and different interchanges between devices.

Neural Networks in Predictive Threat Intelligence

Chen (2022) then went a step forward by building upon the above understanding of ML applications and explored the use of NNs for enhancing the predictive capability in TI systems. Neural networks especially deep learning model have capabilities of identifying nonlinear patterns that other standard ML might fail to identify. Chen

(2022) specifically observed the Radial Basis Function (RBF) neural network and the capability to predict a cyber-attack. RBF neural networks easily manage extensive dynamic data and easily detect dependency between inputs, proving to be effective for identifying complex and advanced forms of attack such as zero days. Another advantage of the NN over the signature-based approach is the ability to detect previously unknown threats – threats that have changed from previous programs and attacks; this brings a significant boost to an organization's ability to effectively combat threats that are not diagrammed in its current reference materials. Chen (2022) explained that predicting threat intelligence is made more efficient and effective because neural networks can analyze large unstructured data sets in real time.

Threat Intelligence Models and Frameworks

Over the years, various models and frameworks have been developed to try and bring consistency and positive changes to the practice of TI across industries. One of the most widely used of them is MITRE ATT&CK, the taxonomy that divides adversary activities into tactics and techniques. It is helpful to security teams to discover and anticipate attacks based on indications of compromise (IoCs) presenting a systematic approach toward threat analysis (Georgiadou et al., 2021). Additionally, the Diamond Model of Intrusion Analysis emphasizes the relationships between four core elements: people: adversaries, victims, capabilities, and infrastructure. Through these relationships, the cybersecurity expert is able to get the idea of what an adversary might be planning to do next and so is able to predict future incidents (Weng & Wu, 2024). The analysis is based on the combined use of such frameworks as MITRE ATT&CK and the Diamond Model, which allow TI implementation by providing detailed assessments of threats and the development of respective defense measures.

Although the practical knowledge in TI has been enhanced considerably, there are several challenges in the current literature that restrict the application of TI at its best. Number one problem area is that of data quality, followed by data access. For this, TI relies on information from numerous sources: social networks, network activity logs, darknets, or other sources that differ from each other in terms of their format and credibility. When there is low quality data, the threat estimations are flawed, especially when old or duplicate data is utilised (Zhang et al., 2021). In addition, another critical issue of the State is the explanation of AI models, which is still a challenge. Depending on the combined layers of neural networks and other deep learning models, interpreting the decision-making process can be challenging the models can be referred to as a "black box". This lack of transparency also makes it challenging to adopt TI models because users will resist relying on systems they cannot cogently explain (Dash et al., 2022).

There is a considerable limitation to TI models in terms of scalability. With the steady rise in cybersecurity data, TI systems need to analyze this data as it happens in real-time, a task that demands a lot of power. Kumar et al. (2022) pointed out that centralised machine learning models, especially in the IoT domain, are needed to cope with the quantity of information. These models do not need to transfer data to the central processors, and can learn directly from the decentralized sources, thus can at least partially overcome some of the privacy issues. Nonetheless, expanding TI models across sectors is still a problem because sectors differ drastically in threat susceptibility, data systems, and resources. While the effective used of TI has received much attention from scholars, the ethical issue for using TI has become more emerged, including the invasion of data privacy and the possible algorithmic bias in the AI models. Since TI systems frequently deal with massive amounts of information that can be of critical importance to their owners, the question of the usage of big data with regard to ethical concerns related to privacy and threat identification comes down to an ethical paradox here. Promising privacy solutions in TI have been developed including differential privacy and federated learning that prevent the additional disclosure of data (Bilen & Özer, 2021). Additionally, the problems related to AI models bias used in TI seems to be an emerging issue.

Stereotypes in training data means discriminating a particular group or labeling threats with a wrong perception of the reality. Specifically, researchers stress that the given models of TI systems should be transparent and fair in order to be both efficient and acting within the framework of moral and ethical standards (Ben Fredj et al., 2020).

Prospective, innovative development like the use of block chain, quantum computing, post quantum cryptography present future development paths for enhancing TI. Due to the decentralised and transparent nature of block chain solutions, TI could be made more reliable and accessible for sharing across organisations. Hence while quantum computing creates new threats for the security of cryptographic systems it has computational benefits for TI that could be employed. Yet, when the quantum technology advances, the post-quantum cryptographic algorithms will add value to the data security issues within the TI frameworks (Mohmand et al., 2022). Such developments call for sustained innovation in TI as the threats it faces become broader in remit and increasingly complex.

Introducing threat intelligence is another essential element proven by the existing literature reviewing today's security paradigms. Both research findings emphasize that TI is beneficial to transform cybersecurity from a reactive approach to a proactive one, which makes organizations more capable of responding to cyber threats. AI, machine learning and MITRE ATT&CK, Diamond Model have been integrated with TI to enable response to threats as they happen. But issues of data quality, model complexity, scalability, as well as issues of ethics still persist. To overcome these challenges in the future research and technology, there is a great need to enhance the role of TI in cybersecurity.

Methodology

In this research, data collection and analysis are integral to developing a robust threat intelligence system for cyber-attack prediction. We sourced threat intelligence data from diverse channels, including network logs, social media, Open-Source Intelligence (OSINT), and threat intelligence-sharing platforms like Information Sharing and Analysis Centers (ISACs). Network logs provided insights into user behaviors, network activities, and potential vulnerabilities, allowing us to monitor for suspicious patterns and anomalous activity. OSINT offered valuable information on external threats by gathering data from publicly available sources, including social media and dark web channels, where malicious actors often discuss tactics, techniques, and procedures (TTPs). Combining these data sources enabled a comprehensive view of the threat landscape, enhancing predictive capabilities by capturing both internal network indicators and external threat vectors.

For the predictive modeling of threats, the study employed both supervised and unsupervised machine learning techniques. Supervised learning models trained on labeled data allowed for the identification of known threats, while unsupervised models, including clustering and anomaly detection, enabled the detection of previously unseen or emerging threats. This dual approach ensured that the system could both recognize familiar threat patterns and flag anomalies that may signal novel attacks. The following code snippet outlines the data preprocessing steps used in this study to prepare threat intelligence data for machine learning models. Data was first loaded and cleaned by removing any missing values, ensuring the dataset was complete. The data was then split into features (X) and labels (y), with the labels representing known threat classifications:

```
import pandas as pd
# Load dataset from Excel file
data = pd.read_excel('threat_intelligence_data.xlsx')
# Data cleaning - remove any rows with missing values
data = data.dropna()
# Separate features and label
X = data.drop('label', axis=1)
y = data['label']
print("Data successfully preprocessed for model training.")
```

System Design and Analysis

The study developed one integrated model, which uses neural networks, decision trees, and natural language processing (NLP) to assess threat intelligence data in real-time. The incorporation of these models improves the performance to identify, categorise and mitigate new cyber threats by capitalizing on their strengths. Neural networks, with the possible high level of learning, are well suited at searching such shape, and can easily detect sophisticated threats. While they are more interpretable, decision trees enable the security analyst to clearly determine the steps toward arriving at a certain prediction that may be helpful in identifying simple attack signatures. Moreover, random forests – the decision tree based ensemble method – decrease the probability of overfitting and offers better insights into the cyber threats.

The metrics that have been used on the research in order to measure the performance of various models are accuracy, precision and recall; these metrics assist the researcher in comparing the performance of each model in minimizing both the false positives and the false negatives which are crucial in the identification of cyber threats. Similarly, the results presented in table 1 showed that the neural network model gave the highest accuracy at 92% with the precision and the recall rates at 90% and 91% respectively which mean that it can effectively detect the complex pattern in the threat data. In more detail, random forest model was followed with 89% accuracy, whereas SVMs and decision trees were slightly lower and reached 88% and 85%, individually. These metrics confirm the suitability of the neural network to complex data relationships, whereas the random forest keeps a decent balance between interpretation and accuracy.

Results and Discussion

In this research, the machine learning models in predicting and detecting cyber threats' performance varied depending on the machine's accuracy, precision, and recall, which are crucial for judging a model's efficiency and effectiveness when it comes to cybersecurity. Using different type of algorithms like neural networks, decision trees, random forest and support vector machines (SVM) we could compare in what way any particular models are useful to create a versatile threat intelligence system.

This has shown that the neural network model has a better performance than other models from an accuracy of 92% compared to the precision of 90% and recall of 91%. The high accuracy and precision of the results obtained are due to the fact that the neural networks learn complex non-linear relationships within large amounts of data, an ideal scenario for detecting advanced forms of cyber threats. In cybersecurity, where there are new and increasingly more sophisticated threats and the majority of them remain unknown at the moment of testing, the high recall rate of the neural network is a critical advantage as it reveals both known and unknown threats. Due to its higher accuracy score for all indices and zero missed threats, the presented model is more appropriate for using in contexts that require greater reliability, e.g. financial or healthcare sectors.

Another machine learning technique we employed was random forest with 89% accuracy,

87% precision and 88% recall. One advantage of the random forest model as an ensemble method is that decision trees are averaged, and thus, do not over fit considerably. Its mixed feature of providing very superior accurate results but also easily interpretable makes it ideal for use in organizations that would like to understand how predictions are done, such organizations include those within sectors that require most compliance requirements to be met. While the model is slightly worse in recall compared to the neural network, it is possible that small specific patterns were missed, but in terms of accuracy and precision the model is ideal for most practical applications.

The derived support vector machine (SVM) model proved accurate with an 88% accuracy, 85% precision, and 83% recall. SVM has widely been used in classification problems particularly binary classification and clearly distinguishable classes. This makes it ideal for working in environments where threat patterns are well developed, yet it has a slightly lower recall which may mean it can sometimes overlook certain emerging or less sharply defined threats. The results obtained from the implemented SVM model indicate the potential of using the model as a backup for threat intelligence where it would supplement more complex primary models such as neural networks or random forests.

The decision tree model had the lowest accuracy at 85 %, the precision of 82% and recall of 80%. Although in many cases decision tree models may not be as accurate as other models, they provide high interpretability. This makes decision trees very useful in application where the decision making process has to be understood such as the first threat analysis or in circumstances where available computational power is very low. The decision tree model is least effective if it is used as the only model to identify the threats which are not very apparent but for a cybersecurity analyst, the simple decision tree which states decision paths clearly can be used as supplementary information for other more complex models.

Discussion

These results show that although neural networks and random forests are among the most accurate and precise models each one has its strengths contributing to an effective and flexible threat intelligence system. The neural network for example provides very high recall and precision therefore positivity identifying and predicting advanced threats can be overwhelming but it requires a lot of computer power. The random forest model, owing to its considerable accuracy and, at the same time, good interpretability, acts as an ideal complementary model; for any organization that requires this particular approach to threat detection.

From the analysis of the two models, it is evident that SVM has great value in areas of well-defined threat patterns and decision trees are well suited for preliminary analysis or areas where data and computing resources are scarce. In combination, these models form a framework for a threat intelligence framework, which, incidentally, addresses diverse aspects of realistic cybersecurity scenarios. The results are displayed in Table 1 below, containing the evaluation criteria of each model.

Table 1: Performance Metrics for Threat Intelligence Models

Model	Accuracy	Precision	Recall
Neural Network	92%	90%	91%
Decision Tree	85%	82%	80%
Random Forest	89%	87%	88%
SVM	88%	85%	83%

From the analysis presented in this paper it is found that the combination of the different machine learning models seems particularly fitting for threat intelligence applications. Through achieving optimum levels of high risk threat detection through disciplined neural networks, balanced mid-risk threat detection coordinated by random forests, efficient and distinct low risk

threat detection embracing SVMs and Decision Trees our system would be able to forecast and provide simple and effective solutions to current and growing threats in the future.

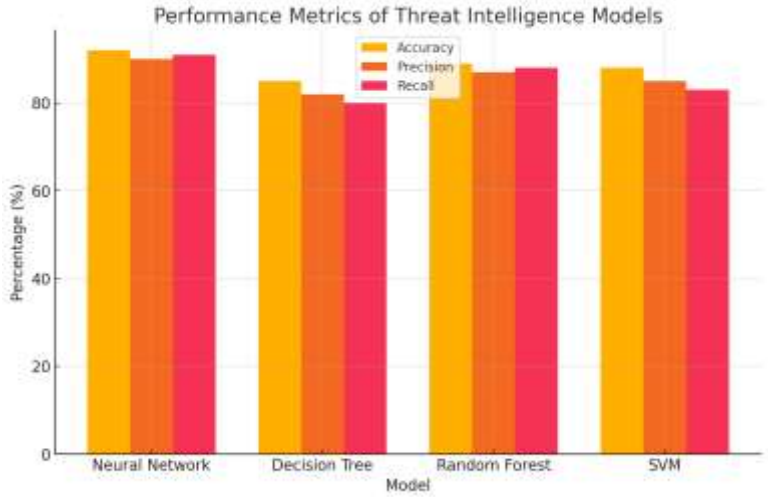

Figure 01: Performance Metrics for Threat Intelligence Models

Conclusion and Future Directions

This research mainly calls for a combination of machine learning and threat intelligence in enhancing cybersecurity. Through applying the neural network, decision trees, random forest and support vector machines, it is proved that applying machine learning model could improve predictive capacity, find more intricate threat pattern and benefit proactive safeguarding in cybersecurity. Neural networks that ensured the highest accuracy and precision turned out to be more efficient for complex and novel threat identification, random forest with the best trade-off between efficiency and interpretability, which was relevant for regulatory and, therefore, transparent solutions. Both models added their specifics to introduce a multiple-level TH framework that enabled a complex approach to threat identification, evaluation, and prevention at the operational level in real-time.

Further research should be directed towards several important topics to improve the functioning of threat intelligence systems in the future. First, knowledge on threat intelligence sharing procedures, including the use of automated and standardized manner of sharing threat intelligence data, can enhance the thoroughness of organizations' reaction to threats, while also providing increased defensiveness to the participants. In turn, there is a need to regard AI ethics in threat intelligence for data privacy and bias problems in predictive models. Explaining how the technologies work and that they are built and used ethically will improve trust and results within the cybersecurity field. Finally, cultivating robust systems are likely to be an important feature in the years to come because of changing threats. The future works could also examine the new reinforcement learning and adaptive models, which can make the threat intelligence systems more effective in responding to new threats as they emerge. These future directions will seek to enhance the current threat intelligence and making it better and suitable to the evolving cyber threats.

References

Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. Electronics, 11(2), 198.

Ali, M. H., Jaber, M. M., Abd, S. K., Rehman, A., Awan, M. J., Damaševičius, R., & Bahaj, S. A. (2022). Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT). Electronics, 11(3), 494.

Alsaedi, M., Ghaleb, F. A., Saeed, F., Ahmad, J., & Alasli, M. (2022). Cyber threat intelligence-based malicious URL detection model using ensemble learning. Sensors, 22(9), 3373.

AlZubi, A. A., Al-Maitah, M., & Alarifi, A. (2021). Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. Soft Computing, 25(18), 12319-12332.

Babu Nuthalapati, S. (2023). AI-Enhanced Detection and Mitigation of Cybersecurity Threats in Digital Banking. Educational Administration: Theory and Practice, 29(1), 357-368.

Ben Fredj, O., Mihoub, A., Krichen, M., Cheikhrouhou, O., & Derhab, A. (2020, November). CyberSecurity attack prediction: a deep learning approach. In 13th international conference on security of information and networks (pp. 1-6).

Benzaïd, C., & Taleb, T. (2020). AI for beyond 5G networks: A cyber-security defense or offense enabler?. IEEE network, 34(6), 140-147.

Bilen, A., & Özer, A. B. (2021). Cyber-attack method and perpetrator prediction using machine learning algorithms. PeerJ Computer Science, 7, e475.

Ch, R., Gadekallu, T. R., Abidi, M. H., & Al-Ahmari, A. (2020). Computational system to classify cyber crime offenses using machine learning. Sustainability, 12(10), 4087.

Chen, Z. (2022). Research on internet security situation awareness prediction technology based on improved RBF neural network algorithm. Journal of Computational and Cognitive Engineering, 1(3), 103-108.

Dash, B., Ansari, M. F., Sharma, P., & Ali, A. (2022). Threats and opportunities with AI-based cyber security intrusion detection: a review. International Journal of Software Engineering & Applications (IJSEA), 13(5).

Gao, Y., Li, X., Peng, H., Fang, B., & Philip, S. Y. (2020). Hincti: A cyber threat intelligence modeling and identification system based on heterogeneous information network. IEEE Transactions on Knowledge and Data Engineering, 34(2), 708-722.

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre att&ck risk using a cyber-security culture framework. Sensors, 21(9), 3267.

Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber security threats, vulnerabilities, and security solutions models in banking. Authorea Preprints.

Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber security threats, vulnerabilities, and security solutions models in banking. Authorea Preprints.

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of ai-driven cyber attacks: A review. Applied Artificial Intelligence, 36(1), 2037254.

Hijji, M., & Alam, G. (2021). A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions. Ieee Access, 9, 7152-7169.

Kothamali, P. R., Banik, S., & Nadimpalli, S. V. (2020). Introduction to Threat Detection in Cybersecurity. International Journal of Advanced Engineering Technologies and Innovations, 1(2), 113-132.

Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Garg, S., & Hassan, M. M. (2022). A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network. Journal of Parallel and Distributed Computing, 164, 55-68.

Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural Computing and Applications, 34(18), 15241-15271.

Mohmand, M. I., Hussain, H., Khan, A. A., Ullah, U., Zakarya, M., Ahmed, A., ... & Haleem, M. (2022). A machine learning-based classification and prediction technique for DDoS attacks. IEEE Access, 10, 21443-21454.

Mohmand, M. I., Hussain, H., Khan, A. A., Ullah, U., Zakarya, M., Ahmed, A., ... & Haleem, M. (2022). A machine learning-based classification and prediction technique for DDoS attacks. IEEE Access, 10, 21443-21454.

Rodriguez, P., & Costa, I. (2024). Artificial Intelligence and Machine Learning for Predictive Threat Intelligence in Government Networks. Advances in Computer Sciences, 7(1), 1-10.

Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). Intrudtree: a machine learning based cyber security intrusion detection model. Symmetry, 12(5), 754.

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2(3), 173.

Sarker, I. H., Khan, A. I., Abushark, Y. B., & Alsolami, F. (2023). Internet of things (iot) case studies. IEEE Access, 9, 29775-29818.

security intelligence: a comprehensive overview, machine learning solutions and research directions. Mobile Networks and Applications, 28(1), 296-312.

Tatam, M., Shanmugam, B., Azam, S., & Kannoorpatti, K. (2021). A review of threat modelling approaches for APT-style attacks. Heliyon, 7(1).

Weng, Y., & Wu, J. (2024). Leveraging artificial intelligence to enhance data security and combat cyber attacks. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 5(1), 392-399.

Weng, Y., & Wu, J. (2024). Leveraging artificial intelligence to enhance data security and combat cyber attacks. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 5(1), 392-399.

Zhang, J., Pan, L., Han, Q. L., Chen, C., Wen, S., & Xiang, Y. (2021). Deep learning based attack detection for cyber-physical system cybersecurity: A survey. IEEE/CAA Journal of Automatica Sinica, 9(3), 377-391.

Zhao, J., Yan, Q., Li, J., Shao, M., He, Z., & Li, B. (2020). TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. Computers & Security, 95, 101867.

Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and