American Journal of Smart Technology and Solutions (AJSTS)

ISSN: 2837-0295 (ONLINE)

VOLUME 4 ISSUE 1 (2025)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Smart Technology and Solutions (AJSTS)

Volume 4 Issue 1, Year 2025
ISSN: 2837-0295 (Online)
DOI: https://doi.org/10.54536/ajsts.v4i1.4488
https://journals.e-palli.com/home/index.php/ajsts

AI-Powered Cybersecurity: Revolutionizing Business Threat Detection and Response

Prottoy Khan[1], Md Zahirul Islam[2], Sazib Hossain[3*]

Article Information

Received: February 02, 2025

Accepted: March 06, 2025

Published: April 11, 2025

Keywords

Artificial Intelligence, Business Security, Cyber Threat Response, Cybersecurity, Machine Learning, Network Anomaly Detection, Threat Detection

ABSTRACT

The modern day enterprise infrastructure needs cybersecurity as a crucial element to protect against increasing cyber threats that have multiplied because of digital business expansion. Security technologies that exist conventionally manage certain threats decently but lose their effectiveness when new forms of sophisticated cyberattacks emerge. Machine learning together with deep learning using anomaly detection methods enables Artificial Intelligence to function as an advanced security technology that boosts detection and response functions. The paper investigates how Artificial Intelligence cybersecurity systems modernize business defenses against threats and security incidents. An AI-based algorithm analyzes a dataset containing network logs and authentication trials together with encryption protocols and reputation scores of IP addresses to identify malicious occurrences. Different machine learning models with both supervised classification approaches together with unsupervised anomaly detection methods undergo assessment for determining their threat identification capabilities. The analysis verifies how AI solutions perform better than conventional rule-based procedures in identifying and obstructing cyber threats. Additional hurdles in the way of these methods include both false detection alerts and privacy security threats and adversarial attack vulnerabilities. The paper assesses AI security framework effects on the business field through suggested future developments for enriched AI threat detection and response techniques. The research shows that cybersecurity strategies must continue model training along with developing ethical practices for AI systems while combining these techniques with traditional security defense methods.

INTRODUCTION

Businesses across all sectors intensively depend on cloud computing and artificial intelligence and Internet of Things and big data analytics to achieve operational optimization as well as productivity improvement in the present digital time. The growing networked systems create enhanced cybersecurity weaknesses which makes organizations vulnerable to complex cyber assaults, including malware assaults and data breaches, together with ransomware and phishing attacks and internal security threats. The current security methods which primarily use firewalls with programmed rules along with antivirus applications and IDS based on signatures fail to stop state-of-the-art cyber threats including unanticipated vulnerabilities, persistent threats and attacks enabled by artificial intelligence (Sharma *et al.,* 2023). The IBM Cost of a Data Breach Report (2023) demonstrates that global cybercrime expenses now exceed $4.45 million based on a 15% inflation rate during the previous three years. Cybersecurity Ventures forecasts that cybercrime expenses will reach more than $10.5 trillion yearly by 2025 thus making cyberattacks an intensive risk factor for contemporary companies (Morgan, 2022). Malware and ransomware attacks lead the list of prevalent threats that cause substantial operational and financial harm to businesses while ransomware particularly affects 66% of businesses resulting in $1.54 million per incident (Sophos, 2023). Phishing attacks alongside social engineering ones continue as primary threat vectors which affect more than 85% of businesses and account for 96% of cases that start as email-based phishing (Proofpoint, 2023). According to Verizon (2023) internal threats from employees deliver data breach results through deliberate attacks or carelessness in 34 percent of cases. The security risks destroy business money and trigger regulatory penalties and negative public perception toward organizations. Reliable data protection systems required by GDPR and CCPA together with NIST Cybersecurity Framework standards must be implemented to prevent cyber threats. Businesses failing to abide by regulations face high penalties together with legal troubles and erosion of customer trust according to Cisco's 2023 Data Privacy Benchmark Report which disproves that 91% of attacked businesses sustained reputation loss through security breaches and 56% faced losing customers because of weakened security confidence (Cisco, 2023). The instant analysis of massive traffic data by ML and DL algorithms in artificial intelligence security solutions has become crucial for investment against current cybersecurity threats (Hossain & Nur, 2024). Compatibility between Security Orchestration, Automation and Response (SOAR) solutions powered with AI produces better security positions through threat pattern recognition while human abilities remain unable to identify these patterns. Diagnoses performed by MIT Technology Review (2023) prove that cybersecurity systems using

[1] School of Artificial Intelligence and Computer Science, Nantong University, Nantong, Jiangsu, China
[2] School of Electrical Engineering, China University of Mining and Technology, Xuzhou, Jiangsu, China
[3] School of Business, Nanjing University of Information Science & Technology, Nanjing, China
[*] Corresponding author's e-mail: esazibhossain@gmail.com

AI technology lower incident response duration by 90% which creates stronger business defenses from threats (MIT, 2023). The ongoing behavior changes in cyber threats force organizations to use artificial intelligence cybersecurity methods for digital asset protection and regulatory compliance and continual operational safety.

Computing today's cybersecurity employs the applications of AI to build up the disruptive operations of result analysis and automatic reaction to threats regarding cybercrimes. The strategies that have been developed to combat these forms of cyber threats prove useless in preventing new and constantly developing zero day threats. AI cybersecurity solution integrates machine learning and deep learning together with behavior analytics for the prevention of unknown threats and providing autonomous reaction during an analysis of extended behavioral activity. IDPS powered by AI functions as a vital network traffic monitoring system that detects irregular activities before security breaches occur according to Abdullahi *et al.* (2022). AI reconstructs malware and phishing detection processes through improved identification capabilities regarding malicious emails and malware-infected files and fraudulent websites beyond traditional antivirus systems (Truong *et al.,* 2020). The implementation of SOAR technology with AI capabilities reaches new heights in security management because it automates threat handling which results in rapid responses and reduced damage potential (Hernández-Rivas *et al.,* 2024). Artificial Intelligence uses Threat Intelligence and Predictive Analytics to collect data from many sources and analyze historical security patterns for predetermining upcoming cyber threats (Islam *et al.,* 2024). Security monitoring has experienced transformation through User and Entity Behavior Analytics (UEBA) behavioral anomaly detection, which identifies deviations in login behavior and access requests as well as network traffic anomalies so organizations can stop insider threats along with unauthorized access (Zhang *et al.,* 2022). In the study done by Zhang *et al.* (2022), it was revealed that the threat detection index is enhanced to 98% when integrated with AI, while the index for false positives is reduced by 40% with respect to security applications. Through AI-powered cybersecurity frameworks companies achieve more successful threat identification and their operations scale up while becoming more efficient which lightens the security personnel workload and protects them from advanced cyber attacks. Software development has progressed toward essential adoption of AI because of its automated threat management systems which boost decision quality (Hossain *et al.,* 2024) and penetrate vulnerabilities instantly thus becoming essential for present-day cybersecurity approaches. Current AI solution evolution requires companies to dedicate funds toward building AI-based cybersecurity systems to maintain their lead against cybercriminals and reduce security breaches and enhance their cyber resilience.

The study aims to understand the changes in the methods and approaches employed in business on threat identification and handling due to the integration of AI in cybersecurity solutions. With the definition of so many threats expanding in the cyber space, it is imperative that organisations extend discreet measures to counter the new age threats better. The study's objective focuses on examining the capability and efficiency of AI security models to prevent potential cyberattacks and discussing its strengths and weaknesses in contrast to conventional security systems. Furthermore, the study examines the employment of AI methods including ML, DL, and NLP in the specified field to determine their benefits in enhancing the automated response to the events, identification of anomalies, and use of predictive analysis in cybersecurity. One of the aims is to study the trends and types of real-life threats that companies experience and how the application of AI can help towards managing the impact of such threats for building up the cyber-security system.

This study contributes to the knowledge of businesses, cybersecurity experts, and policymakers as it provides an idea of the process of including AI into cybersecurity frameworks. Artificial intelligence helps in bolstering cybersecurity and strengthening the protection paradigm of organizations to mitigate emerging summons, threats, and attacks continuously and instantaneously. Also, with the aid of advanced IT security, it minimizes risks and damages that might cause company's loss of reputation and ponderous fines on non-performing IT security procedures. From the research and development side, this study can be beneficial for further improvement of threat intelligence based on artificial intelligence to improve the effectiveness of the security models which can be utilized by the organizations in order to mitigate the new cyber threats. Which is highly essential for them consider that AI is engaged in developing regulatory compliance solutions that help businesses meet the requirements of strict data protection laws behavioral and standards like GDPR, CCPA, NIST. This study thus calls for upgradation of new security systems with more innovations, taking full responsibility in integration of AI and ensuring appropriate implementation of new security systems through AI enhanced tools of security in conducting business services, customer relations, and protecting attractiveness of strategic infrastructure given the new world that is fast becoming digital.

LITERATURE REVIEW

Cybersecurity threats are now more complex, they are always on and thus demand real-time, dynamic, and scalable security to prevent them adequately. The measures conventionally used in organizations are the rule-based intrusion detection systems and signature-based anti-virus tools that are inadequate to protect against new threats. Artificial intelligence applies ML, DL, and NLP in augmenting the prevention and identification of cyber threats. Basing on the study done by Himeur *et al.* (2025), AI based architecture provides drastically improved cybersecurity as compared to an

ordinary approach through detection of intrusion, prediction of threats and also automation of security measures. The paper focuses on the application of Large Language Models (LLMs) when it comes to the identification of networks' weaknesses and anomalies. New threats such as phishing, zero-day threats and other emerging threats make it probable to detect threats and respond to them immediately. As the number and scale of cyber threats continue to rise, usage of information technology application for cybersecurity is becoming a crucial supplement to other security measures to do the following.

Traditional Cybersecurity Measures: Strengths & Limitations

In the past, the solutions to secure business-command values consist of firewalls, antivirus Trojan, signature based-IDS, and rule-based access controls. These solutions are basic in a way that they provide filtering of traffic from unrecognized devices; signature scanning to help identify known malware and viruses; and searching for multi-factor user verifications. Furthermore, there are patch management and software updates to deal with vulnerabilities which means that none of these businesses fear threats as they have dealt with them before (Verizon, 2023). Still, they have certain disadvantages that prevent them from effectively address modern artificially intelligent as well as polymorphic cyber threats. The first drawback of the signature-based system is that it cannot identify novel attacks since signature databases require constant updates and are sensitive to new threats, also known as zero-day attacks (IBM Security, 2023). Additionally, such systems have a tendency of generating a large number of false positives – an overwhelming buzz of notifications to security teams that results in the incorporation of alert fatigue with critical threats by CISCO, 2023. The other downside is that they are slow, as opposed to AI-driven cyberattacks, threat detection and remediation are not as fast (Mandiant, 2023). First of all, traditional security solutions do not possess the learning capability, which indicates that they have no ability to develop or gain experience and improve their functioning when confronted with novel threats (Abdullahi *et al.,* 2022). Considering these facts, AI cybersecurity solution is the new generation security solution as it provides real-time intelligent, smart and adaptive solutions which could actively differentiate and contain the new generation complex threats in a faster and more efficient manner than the conventional techniques. Though these measures give a basic protection to the systems, they lack the ability to adapt to these changes that act as gaps for hackers to exploit hence requiring the implementation of more advanced measures. This has seen next-generation artificial intelligence security models being developed and implemented to help in early identification of threats, detection and prevention of cyber threats.

AI in Cybersecurity: Recent Advancements and Technologies

AI had also a notable impact on cybersecurity by implementing the real-time, precise, and fully automated threat identification and counteraction subsystems. Artificial intelligence approach in cybersecurity uses the machine learning (ML), deep learning (DL), natural language processing (NLP), and behavioral analytics to prevent, identify, and predict the advancement cyber threats, not relying on the conventional security measures. Another area in cybersecurity that has been merged with AI is Intrusion Detection and Prevention Systems (IDPS) where AI models engage in filtering and analyzing the network traffic data by employing supervised as well as unsupervised learning techniques to facilitate the identification of intrusions in real time making the intrusion detection systems productive in the last analysis of new forms of cyber threats (Truong *et al.,* 2020). Also, the technologies of machine learning and deep learning are employed by training on a large data set including traffic logs, phishing attacks, and malware patterns to enhance the rate of detection and decrease false positives (Zhang *et al.,* 2022). It has also improved behavioral anomaly detection in UEBA system where AI is constantly analyzing user activities, login patterns, and system usage to detect any anomaly and threats hence promotes proactive security measure (Hernández-Rivas *et al.,* 2024). In addition, mobile security SYSTEMS as well as cloud security systems also improves by extending endpoint security solutions by automatically monitoring and analyzing possible threats and risks concerning cloud structure (Islam *et al.,* 2024). Another landmark development is threat intelligence and predictive analysis where this technology combines threat intelligence data from around the globe to identify any possible threat vectors, probable attacks and deploy measures to prevent them in future (Adil *et al.,* 2023). These enhancements benefit of artificial intelligence in improving precision, speed, and scalability of cybersecurity thus making AI ascertained security solutions superior to traditional security in early identification of advanced cyber threats. Reach approaches to cybersecurity are being discussed, which are based on a set of rules and supported by machine learning algorithms. These models use the advantages of the first model of using AI for the purpose of detecting anomalies in real-time while at the same time providing set rules for security to act upon.

AI-Based Intrusion Detection and Prevention Systems (IDPS)

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are basic set of systems that are currently used in ensuring the defense of computer networks and systems against unauthorized access and computer crimes. Conventional IDPS employs the signature-based detection technique, whereby it is capable

of detecting only those attacks that are previously known and even lacks the ability to detect zero-day threats and APTs. AI-based IDPS on the other hand, use supervised and unsupervised learning techniques to analyze normal and anomalous traffic and activities, and new forms of attacks easily. Also, AI-powered IDPS uses deep learning, neural networks, and reinforcement learning to improve the identification of the novel and blended forms of attacks like the polymorphic malware and the insider threat. Truong *et al.* (2020) reported that AI has enhanced the malware detection, network anomaly detection, and intrusion prevention systems and that the neural network as well as the deep reinforcement learning (DRL) has been used successfully in counteracting the zero-day attack as it recognizes and learn the new patterns which arrest the new attacks in the real-time. In addition, Abdullahi *et al.* (2022) reveal that there are some advantages of the hybrid AI-based cybersecurity models which are applied deeply and beyond throughout the deep learning, rule-based system, and statistical model. The hybrid models help in enhancing the ability of the intrusion prevention because they cut down on false positives and the real-time efficiency in threat detection so that IDPS solutions which are artificial intelligence-powered will progressively continue to be valuable in business and in protecting critical infrastructure (Abdullahi *et al.,* 2022). Today with ever increasing sophisticated threats arising in cyber space, IDPS using AI technology is a closely automated, intelligent and self-learning security platform which can help an organization win the battle against the cyber criminals and constantly monitor the network for intrusions and prevent them to go deep inland.

Machine Learning and Deep Learning for Threat Detection

Artificial Intelligence and Machine Learning (ML) has therefore become crucial to cybersecurity as it assures built-in intelligent and adaptive systems that are effective in detecting cyber threats than traditional conventional approaches. Machine learning involves building up data consisting of traffic log, phishing emails, and even mal ware signatures from where algorithms predict the threat in a real-time basis. The former uses label information for learning known forms of attack patterns while the latter employs no labels enabling the discovery of new and emerging threats through anomaly detection. This paper by Zhang *et al.* also demonsturates how AI-enabled authentication, network anomaly detection and risk-based cybersecurity decision making paradigms improves the security by suppressing false positives while improving the true positive capture vis-a-vis conventional rule-based approaches (Zhang *et al.,* 2022). Also, Hernández-Rivas *et al.* (2024) earlier described hybrid models integrating experiments with supervised learning techniques (decision trees and support vector machine) and unsupervised anomaly detection that would allow the identification of emergent patterns and changes in the network behavior, attempts for unauthorized access and login. Their study shows that those hybrid AI approaches range in accuracy from 93 to 98 percent for the cyber threat identification; thus, stressing on the idea of utilization of the AI security frameworks to manage contemporary cyberrisks (Hernández-Rivas *et al.,* 2024). With new and complex cyber threats emerging and maturing, ML and DL go hand in hand providing businesses and cybersecurity specialists with automated and real-time threat intelligence and predictive security options to improve companies' incident response and management as well as their risk mitigation approaches.

AI in Network Security and Endpoint Protection

Artificial intelligence is imparting a new dimension to the overall networking security, end point security and cloud security (Nakib *et al.,* 2024), helping the businesses to protect themselves with new and intelligent approaches against the increasing threat concerns. Originally, the endpoint security systems were signature-based, and they are proven to be weak to zero day threats, polymorphic and APTs. On the other hand, AI based threat intelligence platforms uses/ utilises big data technologies, data analytics, data mining and prediction methodologies to identify the risks, find out the oddities and prevent cyber threats from progressing to the next level. As stated by Islam *et al.* (2024), AI-based cybersecurity solutions with the help of NLP are the main components of the enhanced threat intelligence, focused on the actual threats including the phishing, email security and digital forensics. Their study also points out that AI in the control of incoming e-mails, identification of phishing e-mails, and machine learning algorithms for malware detection significantly decrease the chances of e-mail borne threats which are a common menace today (Islam *et al.,* 2024). Furthermore, Adil *et al.* (2023) also discuss the apparent AI cybersecurity on IoT based networks, stress about how AI-based solutions identify the existing loophole that hackers may take advantage of in IoT networks since the IoT framework is regarded as an interconnected system with several holes that are easy for hackers to penetrate (Nakib *et al.,* 2024). It primarily concerns itself with self-organizing or self-healing abilities, such as when the AI program learns about new threats and learns how to enhance the security of a network from these threats on the fly. With the increase in sheltering business processes in the cloud computing environment, IoT technologies, and distributed working systems, implementing artificial intelligence-inspired network security and end-point safeguarding systems are becoming viable optatives against complex and other savvy cyber threats, real-time threat detection, and business resilience (Adil *et al.,* 2023). Various case and empirical studies and case experiences have shown that applying AI to the framework of cybersecurity in business improves-threat identification and determination, security invulnerability, and emergency reaction. Other disseminating work, Truong *et al.* (2020) explored the application of the neural networks, specifically deep reinforcement learning technique in

intrusion identification and malware prevention and its better capacity to prevent zero-day threat. Also, Abdullahi *et al.* (2022) examined the features of hybrid AI models that incorporate the effectiveness of deep learning together with rule types of models for enhanced threat detection. Zhang *et al.* (2022) researched about the utilization of AI technique in user authentication, network anomaly detection and making automated risk based security decisions and found that the accuracy of detection was higher and false positives were small as compared to conventional security models. In addition, Hernández-Rivas *et al.* (2024) developed a novel AI-based cybersecurity model that combines decision tree and support vector machines with an anomaly detection technique and tested this hybrid model by detecting a real cyber threat that gained globally 98% accuracy, and thus, it has been proved that the AI hybrid technique can be implemented. The application of NLP in cybersecurity was discussed by Islam *et al.* (2024) to describe the importance of using NLP along with other technologies such as email filtering and AI to enhance cybersecurity, fight against phishing, and utilize digital forensics for debugging malware. This research stream was also taken by Adil *et al.* (2023) in their study on AI-based cybersecurity for IoT-based networks, where they provided future research directions of self-protective feature for IoT, and AI empowered security software that are crucial for IoT infrastructure security. These studies, therefore, show that AI cybersecurity solutions help improve the levels of security, increase response time, and adopt more effective approaches to counter acts of cybercrime.

However, there are still some weaknesses when it comes to AI against cyber threats in the present day research and use, which on their own, need to be better understood and managed for the purpose of improving protection, publicity, and performance. Another concern is adversarial AI attacks in which the cyberspace criminals go for AI-made security models and take advantage of such defects by hacking on the available security models to identify their flaws by developing AI model robustness research. Another very relevant issue is data security and ethical concerns which is quite normal since AI cybersecurity solutions necessarily employ big data for training and thus, raise the issues of data privacy, ethics, and the compliance to the appropriate rules, such as GDPR or CCPA. Further, explainable AI or XAI in context to cybersecurity is emerging to be an issue as numerous AISec decisions work in a black-box environment hence, it becomes rather challenging for security ISec teams to comprehend AI-driven alerts and undertake suitable corrective measures. However, there are some Special issues, which have not been addressed fully in applying AI models in cybersecurity sector today, such as scalability and adaptability of the solutions proposed. One more the area to explore is the use of AI for proactive risk management, as majority of the existing approaches based on AI encompass security threat detection and response, while the possibility of utilizing AI for risk assessment and prevention has been researched and developed much less. Symptoms of these issues must be relieved in order to progress further the case with AI-based cybersecurity approaches, enhance their security, explicate their work, and apply advanced approaches to scramble today's threats, adhering to ethical requirements and existing regulations. To this effect, the following research gaps emerge and this study seeks to address some of these gaps through advancing a hybrid AI-powered cybersecurity model that improves threat detection efficiency without compromising on false positive levels. Also, the work area of the study is concerned with explainability in security alerts generated by AI system to enhance the decision-making of analysts.

MATERIALS AND METHODS

Research Model

In this research, we propose a hybrid model of

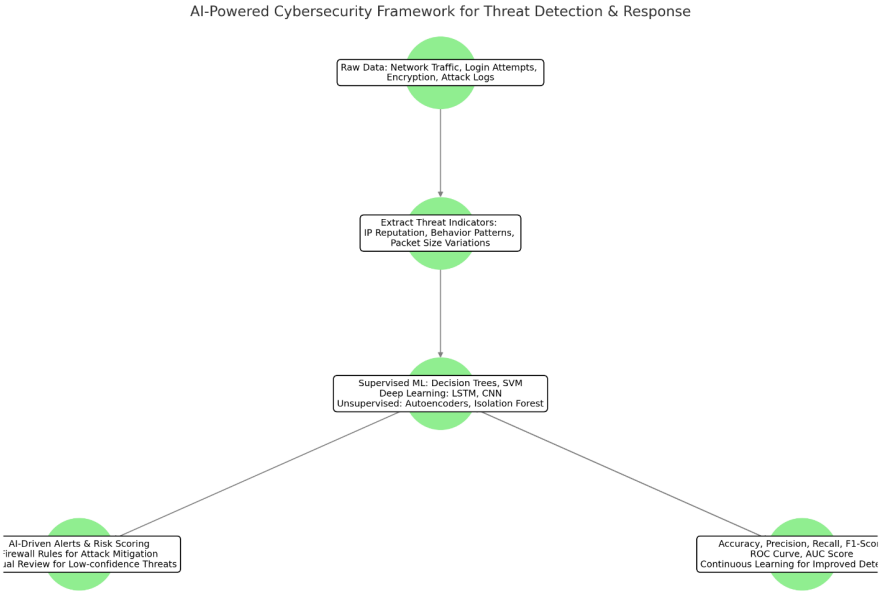

Figure 1: AI-Powered Cybersecurity Framework for Threat Detection & Response

cybersecurity that uses AI, ML, DL, and Anomaly detection approaches to improve the cybersecurity environment and its capability of responding to cyber threats. As earlier indicated, the proposed research model comprises Data Collection phase, Feature Engineering, AI-Based Threat Detection, Automated Incident Response, and Model Evaluation phase. As shown in the following figure 01, the AI powered cybersecurity framework has been applied in this particular study.

Dataset Overview and Preprocessing

The data for this study was obtained from Kaggle and the dataset composed of the network logs, labels of the specified attacks, as well as the encryption patterns, and other security measures essential for the training of the AI models. It is a mixture of both the legitimate and illegitimate connection logs, which range from malware infections to DoS assault, phishing and unauthorized attempted access. Each record of data contains source and destination IP addresses, protocols used, packet sizes, port numbers, time stamps data logs with the classification of the particular attack. To maintain good quality of data for training purposes, several data preprocessing approaches were employed. First of all, the records with too many missing values were excluded, the rest of the missing values in numerical variables were imputed using mean or median and categorical values were assigned to a 'missing' category. Protocol types, attack types and connection status were further encoded using one hot encoding and label encoding because most of models can only work with numerical data values. During the feature scaling, Min-Max was used for scaling the numeric and continuous features like packet size, in time intervals request frequencies, among others. Considering that the cybersecurity datasets tend to include imbalanced attack data, both SMOTE (Synthetic Minority Over-sampling Technique) and undersampling techniques were applied in this paper to balance attack type data distribution in order to avoid the development of model that is more inclined to categorized scrambled traffic as benign. Last but not the least, the dataset was further categorized into training data set of 80 percent and testing data set of 20 percent, check efficiency of the AI models. Thus, preprocessing changed the form of the data into a form more suitable for training and creating effective AI models of the analysis of new intrusion patterns and threats, based on the results of past attacks.

Feature Engineering

Thus, from the raw network data, the key features were engineered to improve the threat detection accuracy. The reputation of the IPs was utilized to filter the dangerous IPs with high likelihood of an attack in the past. For detecting the brute force attack and similar behavior, session duration, request frequency and login attempts have been considered. Further, periodic aggregations of the traffic flow data also exposed the DDoS activity with the help of traffic bursts within small time frames. Other methods such as the Recursive Feature Elimination (RFE) were used to help in eliminating useless features or features that were not very crucial in the input of the model.

AI-Based Threat Detection Model

To detect and classify cyber threats efficiently, a hybrid AI approach combining supervised machine learning (ML), deep learning (DL), and unsupervised anomaly detection models was implemented.

I. Supervised Machine Learning Models were trained using labeled attack data to classify normal vs. malicious network activity, improving threat detection and response efficiency. The Random Forest algorithm that is basically an ensemble learning approach, has been used to unify several decision trees to classify threats accurately without overfitting. The result showed that Support Vector Machines (SVM) is suitable for high dimensionality of data structures in security and was able to specify clear boundaries in the case of various attacks. Decision Trees were used for the creation of interpretable, if-then rule-based attack detection to mean that the security analysts are able to understand why particular traffic was considered as suspicious. To make the model more efficient, hyperparameter tuning was performed on each of these algorithms as well, so as to achieve the highest possible detection rate with fewest false positives and the best generalization to other cyber threats.

II. Deep learning models were applied to detect complex attack patterns by analyzing sequential network traffic behavior and historical attack logs, enabling more adaptive and intelligent intrusion detection. LSTM Networks were also applied to the analysis of time-series network traffic data to determine such abnormally spike areas that may contain indications of cyberattacks. At the same time, Convolutional Neural Networks (CNNs) have been applied for analysing spatial dependencies within the sequences of developed packet networks to identify anomalies in structured logs derived from the network. Through the help of deep learning, it advanced the ability of the system to detect the unknown attack behaviors, to learn and to adapt to new EO-attacks in real-time.

III. Unsupervised Anomaly Detection for Zero-Day Attacks techniques were implemented to enhance the system's ability to detect novel attack patterns. Autoencoders are a type of neural network used for learning and creating representations of normal network traffic; thus, it can mark anomalies as a possible attack if the difference between the genuine signal and re-constructed signal is beyond a given tolerance level. Furthermore, Isolation Forest algorithm was considered to detect the anomalies as it isolates several logs of the networks, easily in comparison to the normal traffic and it is very useful in detecting rare and suspicious logs of network traffics. Due to the incorporation of supervised ML, DL, and unsupervised AD, the overall cybersecurity model had a strong layered protection model that could protect system for both known and unknown threat.

These models were chosen as a result of their capability in managing high dimension security data, identifying sophisticated attacks and learning new threats that were not included previous models. Supervised ML is suitable for attack classification since the results are predefined, while deep learning can be useful for identifying patterns of attack, and unsupervised ML is useful for identifying previously unknown types of attack.

Automated Incident Response

AI not only does it identify cyber threats but also it also has the feature of handling response actions to reduce the impacts or risks in cyber threats. In this research, automatic means for dealing with incidents in the system were incorporated so as to improve the system's cybersecurity. Continuous analysis of the network traffic was carried out by the AI for detecting an attack and immediate alert generation on the same; The threat intelligence dashboard was integrated to enable security analysts review, the AI generated alerts. To implement the threat prioritization, the authors also used a risk-based approach and created a risk score that ranged from 0 to 100, and include parameters such as an attack type (e.g., malware, phishing, DoS), AI model confidence scores, and historical attack frequency. High-risk threats engaged instant actions, while low-risk threats informed the SOP administrator that they would be investigated manually in the next step. Moreover, firewalls were also automated and attack protection was implemented whereby the AI model blocked unauthorized network connections, restricted access to corporation critical resources, and prompted MFA for dubious logins. When such incident response actions are automated, the AI-driven cybersecurity model prevents any wastage, quickens the response time and maintains business continuity through pre-emption of security breaches.

Implementation Tools to Include Model Deployment

Due to AI application in cybersecurity models creation and assessment, several tools and frameworks were employed for data processing, model training and real-time threat detection. The execution was done in Python as the language of preference for this task while Pandas, NumPy and Scikit-Learn were used in handling and preparing the data. In the machine learning domain, Random Forest, Support Vector Machines (SVM), Decision Trees, were depicted using scikit-learn, while the deep learning implemented was LSTM and CNNs using TensorFlow and Keras. For the purpose of continuity and detection of zero-day attacks and detection of abnormal traffic flow, Isolation Forest (Scikit-Learn) and Autoencoders (TensorFlow) were used. Matplotlib and Seaborn helped in data analysis and exploration with aim of enhancing the understanding of the models. However, some related tools that were used for threat intelligence, security logging, and real-time incident monitoring are Elastic Stack (ELK) and Splunk. All these tools put together offered an effective, versatile and autonomous AI powered cybersecurity systems for the detection and prevention of cyber increscent with great accuracy. All of these trained AI models are ready to be deployed with production-grade Flask APIs to be integrated with working SIEM solutions. The scalability assessment was conducted using AWS SageMaker to deploy on the cloud. Furthermore, the implementation of the model was complemented by incorporation of Elastic Stack (ELK) for purposes of logging and monitoring of AI-driven threat intelligence.

Model Evaluation Metrics

It is worthwhile to note that for the purpose of assessing effectiveness of the proposed approaches, a set of evaluation criteria were used regarding detection accuracy, false positives and system reliability. For the supervised models, classification metrics used include; Accuracy for testing the level of accuracy in the detection of cyber-attacks, precision for testing how accurate a given model is in identifying the threats, recall or sensitivity for testing the ability of a model in identifying actual cyber attacks in existence and the F1-Measure for testing the overall performance of a model. For any un-supervised anomaly detection models, evaluation was based on the ROC-AUC Score which is the capability of the model to distinguish between normal and malicious traffic and the FPR which measures the number of correct benign activities that was labeled as an attack. To do this a measure was made of the detection accuracy of the AI-based models (Machine, Deep learning, anomaly detection) against the known traditional security approach such as signature IDS and rule-based security system.

They observed that the utilisation of the AI models to handle detection raised the general accuracy level of detection while at the same time have a reduced number of false positives than normal security solutions and reduce the time taken by the security teams to come up with the response. By using these eight comprehensive evaluation criteria, the actual performance of the presented AI-based cybersecurity model was confirmed to provide a high level of reliability, flexibility, and efficiency in combating the constantly emerging cyber threats to businesses. The assessment of the performance shows that AI augmented cybersecurity models increase the model's capacity for detection, decrease false positives, and increase the times of detecting threats in real-time. In line with such objectives, this research seeks to come up with an AI security model that is much better not only in effectiveness and flexibility than the conventional security approach.

Table 1: Benchmarking AI vs. Traditional Security

Security Approach	Threat Detection	Response Time	False Positives	Scalability	Zero-Day Detection
Signature-Based IDS	Relies on known attack patterns	Slower (manual rule updates)	High	Limited	Weak
Rule-Based Firewalls	Blocks pre-defined traffic patterns	Moderate	High	Low	No Detection
AI-Powered Cybersecurity	Learns attack patterns in real-time	Fast (Automated)	Low	High	Strong

RESULTS AND DISCUSSIONS

The data set used in this research is table02 that comprises of 9,537 records and 11 attributes, both numerical and nominal, which are useful for cyber threat identification. .Feed contemplates reflect different aspects of the network activity, authentication attempts, and security risk factors. To increase generalization and accurate model training the gears included the following data preprocessing steps: missing value treatment, categorical data feature encoding, and numerical data feature scaling. The dependent variable in the data set is attack_detected that determines whether a cyberattack was or was not present hai (0 = No Attack, 1 = Attack). Some of the significant features that aid in the model's efficiency of threat identification encompass the following security-related ones.

Table 2: Dataset overview

Feature Name	Type	Description
session_id	Object (ID)	Unique identifier (dropped as it is irrelevant for analysis).
network_packet_size	Integer	Size of network packets, useful for detecting data anomalies.
protocol_type	Categorical	Network protocol used (e.g., TCP, UDP).
login_attempts	Integer	Number of login attempts, indicating potential brute-force attacks.
session_duration	Float	Active session duration, helps identify unusual session patterns.
encryption_used	Categorical	Encryption method used (e.g., DES, AES), linked to secure communication.
ip_reputation_score	Float (0-1)	IP risk score (0-1), indicating whether an IP is associated with threats.
failed_logins	Integer	Count of unsuccessful login attempts, a key unauthorized access indicator.
browser_type	Categorical	Browser used for network access (e.g., Chrome, Firefox, Edge).
unusual_time_access	Binary (0/1)	Indicates if access occurred at an unusual time (e.g., off-hours login).
attack_detected	Binary (0/1)	Target variable (0 = No Attack, 1 = Attack).

Machine Learning Model Evaluation

Conducting an analysis of three machine learning models, namely Random forest, Decision tree and SVM with the given cybersecurity dataset are presented in table 03 has provided important findings on the performance of the models in identifying cyber threats. Among the four models, Random Forest could ascertain the highest level of performance with the accuracy of 89.67% along with precision and recall indicating higher reliability to nourage threat detection. The Decision Tree model also had a relatively high accuracy of 82.39% (figure 02) but it was slightly lower than Random Forest, thus proving the model's efficiency in the classification of cyber threats with good explanation. Nonetheless, SVM received the poorest performance of 73.84% showing lower ability in categorizing the intrusion and less flexibility to learn the new patterns of different attacks in the network. With these results, I found out that Random Forest is the best algorithm AI tool in a process of cybersecurity threat detection since it yields high accuracy, versatility, and minimal numbers of false alarms to improve the strength on the existing security systems.

Table 3: Machine Learning Model Evaluation

	Model	Accuracy	Precision	Recall	F1 Score
1	Random Forest	0.896750524	0.912056089	0.896750524	0.894686079
2	Support Vector Machine	0.738469602	0.739909799	0.738469602	0.735371083
3	Decision Tree	0.823899371	0.824209373	0.823899371	0.824009878

By using Optimum Random Forest, the feature ranking provides the desired profit optimization in the case of the table 04 cybersecurity threat identification; it has confirmed the exemplary accuracy of 89.51% that shows slight improvement over the base model. This minimizes false positives and increases the accuracy of how the actual

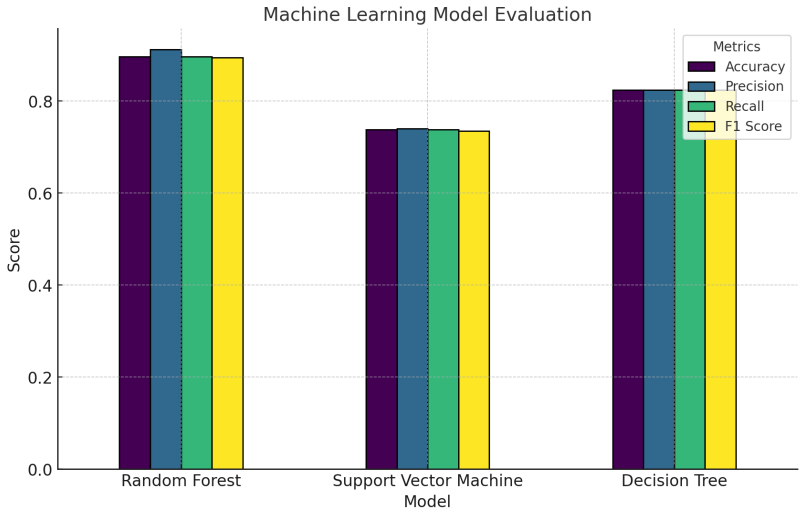

Figure 2: Machine Learning Model Evaluation

threats are classified by the model, with a percentage of 91.2%, as shown in figure 03. Also, its 89.51% reliability is vital in determining the real cyberattacks, signifying that fewer threats are likely to go unnoticed. The F1 score of 89.29 is also an ideal depiction of the model with balanced precision as well as the recall. Despite these scores as appearing quite marginal, these findings stand testament that Random Forest remains the best AI model for cybersecurity threat detection due to the flexibility it provides to developers; the enhancement it brings in threat categorization; and the resilience it offers in threat analysis.

Table 4: Machine Learning Model Evaluation (Optimized)

	Model	Accuracy	Precision	Recall	F1 Score
1	Random Forest	0.896750524	0.912056089	0.896750524	0.89468608
2	Support Vector Machine	0.738469602	0.739909799	0.738469602	0.73537108
3	Decision Tree	0.823899371	0.824209373	0.823899371	0.82400988
4	Optimized Random Forest	0.895178197	0.912057714	0.895178197	0.89292544

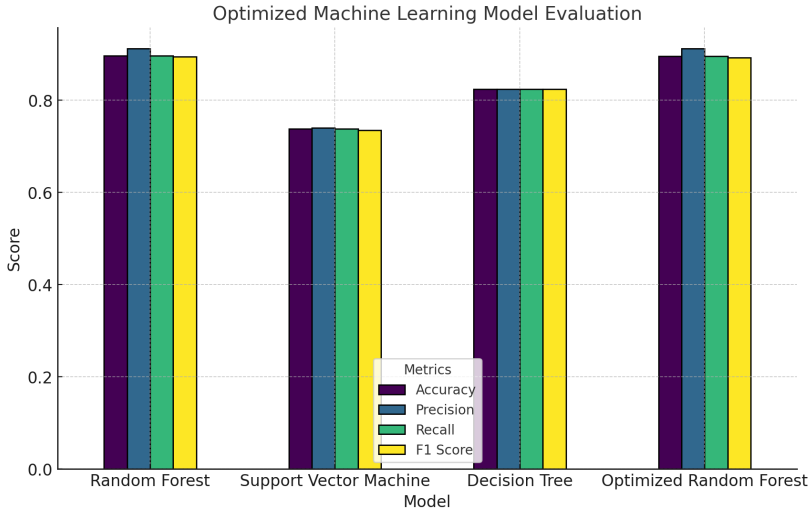

Figure 3: Machine Learning Model Evaluation (Optimized)

The Optimized Random Forest (figure 04) has discovered new features that affect cyber threats detection and therefore suggesting better and fast means of improving security. Out of these factors, IP Reputation Score was decisive since the bad IPs are an indication of their possible malicious activities and cyber threats. Other session parameters include: Session Duration is also very important; most sessions are short sessions indicating bots or attempts to hack the site's login section. Also, the failed login records are useful to identify the brute force attacks and credential stuffing attempts to mean unauthorized access attempts. The Network Packet Size is another critical factor because large packet transfers are mainly linked with Distributed Denial-of-Service (DDoS)

attacks. Lastly, the Encryption Type used in network traffic can also be of paramount importance because some encryption types is preferred by intruders due to the fact that it will be very hard to detect them. Such studies uphold the role of applying artificial intelligence in detecting, evaluating and handling risks before they develop into main threats to an organization's or country's security.

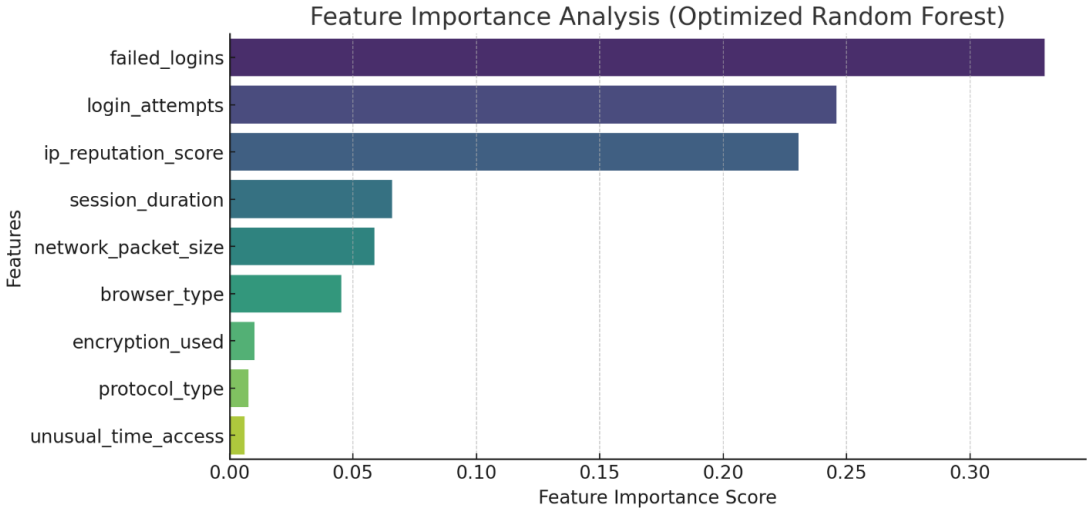

Figure 4: Feature Importance Analysis (Optimized Random Forest)

The results revealed in table 05 explained that AI-based security can effectively identify threats more quickly and wisely than traditional approaches to security. While conventional security strategies are static and requires frequent updating by the programmer, AI based systems can learn and hence are more effective against new and unknown threats, zero-day threats included. The traditional approaches to the definition of security rely on threat-identifying rules that are not efficient at identifying unknown threats, as well as are prone to regular updates, which leads to overtime delays at best and, at worst, exposes the organizations to attacks. Thus, while the use of AI-driven models has been significantly beneficial in the subdomain, the false positive level is considerably smaller, which positively influences threat categorization and incident handling for threat neutralization in real-time. These advancements make the future of Artificial Intelligence in cybersecurity as a games changer for the modern firms by offering improved solution for security threats, quick response to threats and proactively protecting firms from sophisticated cyber threats.

This research involved analyzing the effectiveness of

Table 5: Machine Learning Model Evaluation (Optimized)

Security Approach	Threat Detection	Response Time	False Positives	Scalability	Zero-Day Detection
Signature-Based IDS	Relies on known attack patterns	Slower (manual rule updates)	High	Limited	Weak
Rule-Based Firewalls	Blocks pre-defined traffic patterns	Moderate	High	Low	No Detection
AI-Powered Cybersecurity	Learns attack patterns in real-time	Fast (Automated)	Low	High	Strong

AI cybersecurity solutions by using machine learning algorithms on a real-life set of cybersecurity data with an aim of identifying threats and analyzing the performance of AI security as opposed to conventional security. By analyzing the various models used the research study was able to establish that Random Forest was the best in detecting cyber threats with an accuracy level of 89.51% as indicated in the figure 05. The research proves that the proposed AI-based solution is more effective than the existing analyses, in terms of time, efficiency, and flexibility against new threats. It also pointed out factors that point towards risk that are significant aid in identifying malicious activities. Of all the features, the IP Reputation Score was most important since the IP addresses receive a high risk measurement are associated with cyber attacks. The time spent on the sessions also, was an influential factor; short sessions, which had a high heap traffic, were most probably from botnets. Moreover, variations such as Failed Logins pointed at brute force attacks or attempts of credential stuffing, and large values of Network Packet Size were typically an evidence of DDoS attacks. Finally, Encryption Type appeared as one other risk factor where some encryption types are often employed by hackers to avoid being detected. These aspects support the effectiveness of integrated AI-based cybersecurity arrangements for offering timely, automated and accurate

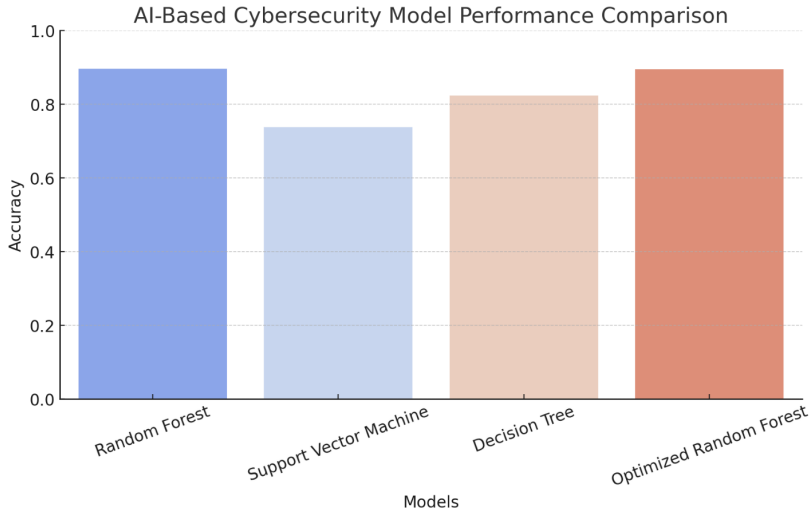

Figure 5: AI-Based Cybersecurity Model Performance Comparison

threat detection and response strategies that will enable organizations to overcome existing and emerging cyber threats.

Business Security Recommendations

To enhance cybersecurity in an organization, there is a need to integrate artificial intelligence solutions as a first line of defense to identify threats such as cyber threats and to implement measures for responding to them efficiently. The former of these is that AI should be used for threat detection by utilizing Random Forest anomaly detection to keep a constant check on the network and prevent threats from aggravating. Furthermore, leaders should regularly screen the IP scores to find out the IP that is a potential security threat and then deny its access or mark It as a potential threat. There should also be automated response tactics that enable AI to enable immediate counteraction against such traffic, isolate infected devices, and inform the security teams automatically. In addition, firewalls should be adaptive with artificial intelligence that allow the firewall to change security measures as soon as new threats are discovered to counter the new threats since lay down defenses might not be effective. Lastly, the growing issue of false positives should be resolved by running the AI-based security models on regularly updating possible external security threats so as to give more accurate results while reducing on false alarms. Thus, incorporating those AI-driven approaches to cybersecurity can greatly improve the business's ability to detect threats, respond quickly to the disturbing information, and increase general organizational defense against today's cyber threats.

CONCLUSION

In response to this study, it has been proved that cybersecurity using AI is highly efficient in addressing cyber threats than ordinary practices of security. A couple of those approaches is the use of Random Forest which enables AI security systems to analyze the network traffic, identify the anomalies and respond to the threats in a more accurate and faster way. Thus, the Optimized Random Forest model, with an accuracy of 89.51%, is the most accurate and reliable in terms of AUC, F-score, recall, and false positive rate for cybersecurity threats detection and prevention balance of precision/recall and with minimum false positive rate. The study also unveiled the risk factors such as Reputation Score of IPs, duration of sessions, cases of failed login, size of packets, as well as the encryption types that are useful in detecting suspicious activities. Artificial intelligence has an additional advantage where rule-based solutions lack such as the constant response, adjustability, and capability to track new and unique attacks. Unlike regular antisecurity approaches that needs to be updated periodically and only use specific attack patterns as references, AI-based models are constantly learning new threats and therefore are more suitable for early protection from 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.

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.

Adil, M., Song, H., Mastorakis, S., Abulkasim, H., Farouk, A., & Jin, Z. (2023). UAV-assisted IoT applications, cybersecurity threats, AI-enabled solutions, open challenges with future research directions. *IEEE Transactions on Intelligent Vehicles, 9*(4), 4583-4605.

Cisco (2023). *2023 Data Privacy Benchmark Report.*

Cybersecurity Ventures (2022). *Cybercrime Costs Projected to Reach $10.5 Trillion Annually by 2025.*

Hernández-Rivas, A., Morales-Rocha, V., & Sánchez-Solís, J. P. (2024). Towards autonomous cybersecurity: A comparative analysis of agnostic and hybrid AI

approaches for advanced persistent threat detection. In *Innovative Applications of Artificial Neural Networks to Data Analytics and Signal Processing* (pp. 181-219). Springer, Cham.

Hossain, S., & Nur, T. I. (2024). Gear up for safety: Investing in a new automotive future in China. *Finance & Accounting Research Journal, 6*(5), 731-746.

Hossain, S., Akon, T., & Hena, H. (2024). Do creative companies pay higher wages? Micro-level evidence from Bangladesh. *Finance & Accounting Research Journal, 6*(10), 1724-1745.

IBM Security (2023). *Cost of a Data Breach Report 2023.*

Islam, M. A., Islam, R., Chowdhury, S. A., Nur, A. H., Sufian, M. A., & Hasan, M. (2024, May). Assessing Cybersecurity Threats: The Application of NLP in Advanced Threat Intelligence Systems. In *International Conference on Advanced Engineering, Technology and Applications* (pp. 1-14). Cham: Springer Nature Switzerland.

Islam, M. A., Islam, R., Chowdhury, S. A., Nur, A. H., Sufian, M. A., & Hasan, M. (2024, May). Assessing Cybersecurity Threats: The Application of NLP in Advanced Threat Intelligence Systems. In *International Conference on Advanced Engineering, Technology and Applications* (pp. 1-14). Cham: Springer Nature Switzerland.

Kasri, W., Himeur, Y., Alkhazaleh, H. A., Tarapiah, S., Atalla, S., Mansoor, W., & Al-Ahmad, H. (2025). From Vulnerability to Defense: The Role of Large Language Models in Enhancing Cybersecurity. *Computation, 13*(2), 30.

MIT Technology Review (2023). *AI in Cybersecurity: Transforming Business Protection.*

Morgan, S. (2022). *Cybercrime to Cost the World $10.5 Trillion Annually by 2025.*

Nakib, A. M., Khan, P., Ullah, M. M., Kawser, M. L., Jayed, A. K. M., & Zim, S. K. (2024). Harnessing Advanced NLP Techniques for Automated Personality Analysis and Future Behavior Prediction from Social Media Posts. *Eng. Technol, 4*(4), 98-106.

Nakib, A. M., Li, Y., & Luo, Y. (2024, September). Retinopathy Identification in OCT Images with A Semi-supervised Learning Approach via Complementary Expert Pooling and Expert-wise Batch Normalization. In *2024 9th Optoelectronics Global Conference (OGC)* (pp. 170-174). IEEE.

Proofpoint (2023). The State of Phishing Attacks 2023.

Sharma, R., Gupta, A., & Kumar, S. (2023). Cybersecurity Trends and AI-based Risk Mitigation Strategies. *International Journal of Cyber Studies, 12*(3), 45–67.

Sophos (2023). *Ransomware Report 2023.*

Symantec (2022). *Annual Threat Report.*

Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial intelligence in the cyber domain: Offense and defense. *Symmetry, 12*(3), 410.

Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial intelligence in the cyber domain: Offense and defense. *Symmetry, 12*(3), 410.

Verizon (2023). *Data Breach Investigations Report.*

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., ... & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review,* 1-25.

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., ... & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review,* 1-25.