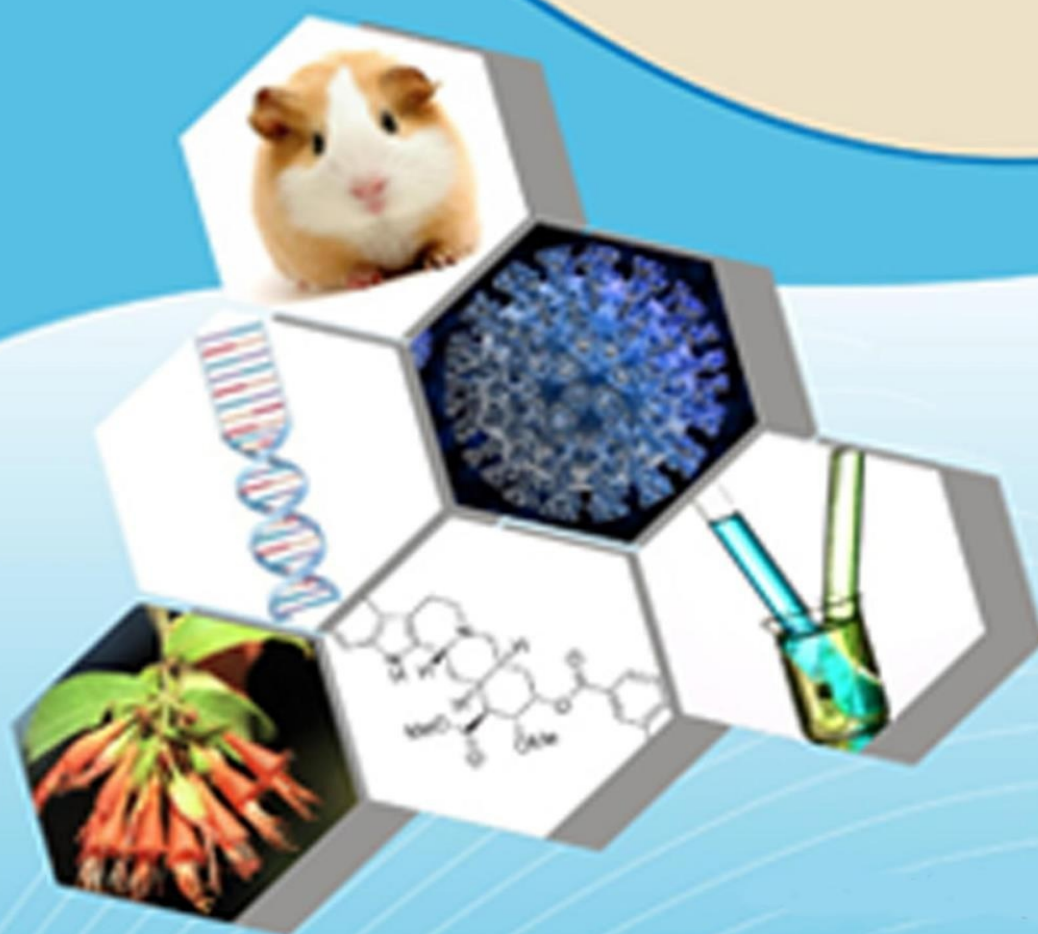




ISSN : 2347-2251
**Indo-American Journal of
Pharma and Bio Sciences**



www.iajpb.com

iajpb.editor@gmail.com
editor@iajpb.com



AI-POWERED CYBER THREAT DETECTION AND RESPONSE: LEVERAGING NETWORK, TEXTUAL, AND RELATIONAL DATA

¹Venkat Garikipati

Innosoft, Maryland, USA

venkat44557@gmail.com

²Charles Ubagaram

Tata Consultancy Services, Ohio, USA

charlesubagaram17@gmail.com

³Narsing Rao Dyavani

Uber Technologies Inc, California, USA

nrd3010@gmail.com

⁴Bhagath Singh Jayaprakasam

Cognizant Technology Solutions, Texas, USA

Bhagath.mtech903@gmail.com

⁵Rohith Reddy Mandala

Tekzone Systems Inc, Rancho Cordova,
California, USA

rohithreddymandala4@gmail.com

⁶R. Mekala

Sri Ranganathar Institute of Engineering and Technology
Coimbatore, India.

mail2dr.mekala@gmail.com

ABSTRACT

To address the acute security threats, there has been a movement toward deep learning techniques to automate and supplement threat detection and response systems. Modern sophisticated attacks like Advanced Persistent Threats (APTs), malware, and phishing are eluding detection by traditional rules and signatures. This study examines Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) in classifications and interesting to note that the same is studied regarding their detection of malicious behaviour across diverse datasets in cybersecurity. The study intends to go further to examine deep learning models used in real-time monitoring, classification, and incident response of network traffic logs, system logs, user activity logs, and malware samples. The paper will also highlight the impact that exercises such as normalization, Z-scoring, and data imputation for the improvement of model performance can have on the results. Key challenges considered by the paper to affect the AI systems concerned are issues faced with scalability, data imbalance, and adaptation to novel threats. A comparison study indicates the development of hybrid models and real-time detection systems, shedding light on how deep learning could be used to design more adaptable, resource-efficient, and effective cybersecurity solutions. The evolution of models from feedback loops will also run through the paper.

Keywords: Deep Learning, Threat Detection, Automated Response, Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Cybersecurity

1.INTRODUCTION

The last few years have seen a growing trend through which the use of deep learning has been characterized by online automatic identification and responses toward threats, mainly due to the complexities involved in processing a wide variety of forms of data and high-dimensional data [1]. On their end, traditional cybersecurity systems rely on signature-based and rule-based methods to keep up with the life of their threats, including but not limited to Advanced Persistent Threats (APTs), malware and phishing attacks among many others that find ways



to bypass any traditional defences [2]. Such deep learning models have thus emerged as superior in proving the CNNs and the RNNs as specific types in that they are better placed in an automatic pattern learning exercise from the raw data [3]. Real-time monitoring, classification, and incident response in these models provide the flexibility and scalability required for adaptive analysis to the detection processes and mitigation of cyber threats in a very dynamic environment [4].

This document talks about applying deep learning techniques, particularly CNN and RNN, in classifying and detecting threats within cybersecurity [5]. It discusses how deep learning models can be trained to identify many threat types, from malicious network traffic to malware detection [6]. The data used in the training has its origins in different kinds of logs, such as network traffic logs, system logs, and logs about user activity and even malware samples, among others [7]. It also highlights critical data pre-processing strategies, including normalization, Z-scoring, and data imputation at their depth, which are important for improving performance in producing a deep learning model [8]. Deep learning techniques, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), are becoming increasingly essential in the field of cybersecurity due to their ability to handle vast and complex data in real-time [9]. Traditional cybersecurity systems often rely on signature-based or rule-based detection methods, which can be bypassed by sophisticated and ever-evolving cyber threats such as Advanced Persistent Threats (APTs), malware, and phishing attacks [10]. Unlike these conventional methods, deep learning models are capable of learning directly from raw, high-dimensional data, allowing them to automatically identify patterns, anomalies, and potential threats without relying on predefined rules or signatures [11]. This makes them highly effective in detecting new, unknown attacks, and adapting to changing attack strategies in dynamic environments [12].

Deep learning models are trained on diverse data sources, including network traffic logs, system logs, user activity logs, and even malware samples [13]. These data types provide critical insights into potential malicious activities, and when fed into deep learning models, they enable automatic pattern recognition and behavior analysis [14]. CNNs are particularly well-suited for detecting patterns within static data, such as identifying anomalies in network traffic or malware signatures, while RNNs excel in analyzing sequential data, like time-series logs, to identify deviations in user behavior or network activities [15]. The combination of these techniques enhances the ability to detect both known and novel threats, offering superior threat detection capabilities compared to traditional approaches [16].

Effective data preprocessing is crucial to ensure that deep learning models achieve optimal performance [17]. Techniques such as normalization, Z-scoring, and data imputation help clean and standardize the input data, ensuring that it is consistent and ready for training [18]. These preprocessing steps improve the quality of the data, which, in turn, enhances the accuracy of the model's predictions [19]. By training on well-preprocessed data, deep learning models can identify subtle threats more effectively, reduce false positives, and ensure that incident responses are both accurate and timely. In real-time applications, these models can continuously monitor systems, flag suspicious activity, and even initiate automatic responses to mitigate the impact of detected threats, offering a scalable and adaptive solution to cybersecurity challenges [20].

2.PROBLEM STATEMENT

AI has been faced with numerous challenges regarding cyber security [21]. These challenges are particularly in terms of scalability, data imbalance, and adapting to new emerging threats [22]. One of the serious issues is the scalability of models that can be scaled up to increasing amounts of data in real-time environments [23]. Network traffic is only going to increase and become more complex, and it becomes hard, if not impossible, to train and deploy AI models efficiently [24]. While earlier researchers have taken distributed computing and cloud solutions to be the old methods of scaling AI models, these do not scale well in real-time threat detection [25]. Nowadays, the focus has advanced to build better architectures and computationally efficient approaches [26].

The problem of data imbalance is one area of concern because, like consumer banks, an organization has far more benign activity instances compared to the malicious ones [27]. Earlier traditional methods like oversampling, under sampling, and cost-sensitive learning mostly end up overfitting or underfitting a given model [28]. Recent generative models and hybrid techniques are, however, being studied with the aim of being able to leverage their greater generalization ability to really contend against class imbalance [29]. Not only that but AI models also continuously adapt to new emerging threats like the APT. Earlier methods made the input in the model for retraining it and allowed it to learn new possible attack signatures [30]. However, the recent one emphasizes online learning and transfer learning while allowing the models to be updated with real-time acquisition of new attack



patterns. Another major challenge is the high false-positive and false-negative rates characteristic of most AI-driven systems. The earlier studies, while second classifying through this rate, offered manners.

3.OBJECTIVE

- AI-powered model of data fully explored for cybersecurity especially such as CNN and SVM in threat classification and detection task.
- To create a machine learning model is capable of identifying benign and malicious behaviors. based on various intrusion detection datasets, such as the combination of network traffic logs, system logs, user activities, malware samples, and IDS outputs.
- To transform the data using a series of pre-processing techniques including Z-scoring, normalization, and data imputation to prepare them for a machine learning model and have compatible features with equal contribution to the learning process.
- PCA Application for Feature Extraction for Dimensionality Reduction and Preservation of Variance to Enhance Efficiency in the Model for Detection of Threats.
- To measure the performance of the CNN-based threat detection models based on the automated feature acquisition from raw data and classifying threats in cyber datasets.
- Deploy machine learning models trained into live cyber defence systems, for example: firewalls, intrusion detection systems and security information and event management systems to monitor for and respond in real time to emerging threats.
- Assess and evolve periodically the performance of deployed models through feedback loops for the effective detection of new and evolving cyber threats.

4.LITERATURE SURVEY

AI-driven cybersecurity systems have gained traction, with Convolutional Neural Networks (CNNs) and Support Vector Machines (SVMs) being widely used for automating the process of cyber threat recognition and mitigation [31]. These models have demonstrated significant potential in improving threat detection accuracy compared to traditional methods [32]. For example, CNNs, through the stacking of hierarchical features from raw packet data, have proven effective in enhancing the detection of Distributed Denial of Service (DDoS) attacks and malware, surpassing older models such as k-Nearest Neighbours (k-NN) and Random Forest [33]. When employed in Intrusion Detection Systems (IDS), CNNs have also demonstrated lower false positive rates and higher detection performance, making them a promising solution for identifying network intrusions and other malicious activities [34]. SVMs, known for their ability to handle high-dimensional data, have been particularly effective in phishing detection and bot detection [35]. Their application in classifying malicious network traffic has shown that they can efficiently separate benign from malicious data [36]. Combining CNNs with SVMs in hybrid models has become an increasingly popular approach, especially in tackling more sophisticated threats such as Advanced Persistent Threats (APTs) [37]. These hybrid models leverage the feature extraction capabilities of CNNs along with the classification strengths of SVMs, resulting in enhanced performance compared to standalone models [38]. Such models are particularly well-suited for the dynamic and evolving nature of modern cyber threats [39].

The field of AI-driven cybersecurity is continuously evolving, with recent studies focusing on improving the scalability, efficiency, and adaptability of machine learning models [40]. Despite the effectiveness of CNNs and SVMs in classifying network traffic and identifying malware or phishing attacks, challenges such as model scalability, data imbalance, and the ever-changing landscape of cyber threats remain prevalent [41]. Researchers have increasingly turned to hybrid models that combine ensemble methods with CNNs and SVMs, further enhancing classification accuracy and robustness [42]. Additionally, the integration of techniques like transfer learning and online learning allows for models to adapt seamlessly to emerging trends without the need for complete retraining [43]. With continuous feedback loops for learning from new labeled data, AI models in cybersecurity are becoming more efficient, adaptive, and responsive to new threats, signalling a shift toward more dynamic and resilient security systems in the future [44]. The integration of deep learning models, particularly Convolutional Neural Networks (CNNs) and Support Vector Machines (SVMs), in cybersecurity has brought forth substantial advancements in threat detection and response [45]. These models excel in handling large and complex datasets, which are essential in identifying and mitigating sophisticated cyber threats [46]. CNNs are especially effective in extracting hierarchical features from raw data, allowing them to detect patterns and anomalies in network traffic and malware signatures [47]. Meanwhile, SVMs are commonly used for their ability to classify high-dimensional data, making them highly efficient in tasks such as identifying phishing websites or distinguishing between legitimate and malicious traffic [48]. The combination of both techniques into hybrid



models has further increased their capabilities, providing more precise and scalable solutions for advanced threat detection.

Despite the promising results achieved by deep learning models, challenges remain in their application to cybersecurity. Issues such as data imbalance, where there is a disproportionate amount of benign versus malicious data, continue to affect model accuracy and performance [49]. Additionally, the rapidly evolving nature of cyber threats requires models to be flexible and adaptive. Recent developments in hybrid models, which combine CNNs and SVMs with other techniques like decision trees or ensemble methods, have shown promising results in tackling these challenges [50]. These models are designed to improve both classification accuracy and robustness by leveraging the strengths of different algorithms [51]. This hybrid approach has proven effective in enhancing cybersecurity defenses, particularly against more complex and stealthy threats, such as APTs.

5.PROPOSED METHODOLOGY

Data collection in gathering information from an array of cybersecurity source materials such as network traffic logs, application logs, user activities, and malware samples which is very much needed for training the classification models. Then comes pre-processing, which includes normalization to put all features on a specific range; Z-scoring applies zero mean and unit variance standardization to all features; and imputation of missing values using either average replacement techniques or k-NN imputation. The next step is feature extraction via Convolutional Neural Networks (CNNs), best suited for learning intricate patterns from high-dimensional data like network traffic or time series data by converting them into grid-like structures. Classification follows the extraction of features; it is the Support Vector Machine (SVM) that classes the data, where SVM seeks to find the best hyperplane in the feature space so that the different threats (benign versus malicious, for example) may then be well classified. Then identification leads us into the security deployment phase, which follows. where the trained model is employed for combating emerging threats in real-time within a real-world environment. Finally, the evaluation of performance uses accuracy, precision, recall, F1-score, etc., to test the effectiveness of the system and further goes for continuous testing and fine-tuning in response to feedback to increase its detection capability.

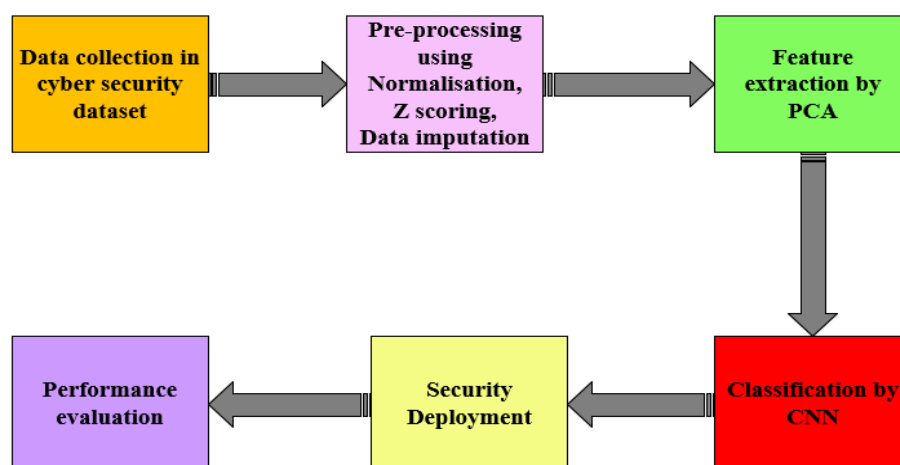


Figure 1: Workflow for Cybersecurity Threat Classification Using PCA and CNN

DATA COLLECTION IN CYBERSECURITY DATASET:

The datasets collected for this research will help create a course in a machine learning model for threat classification and detection. The data sources for these datasets would include network traffic logs, system logs, and logs about user activity, malware samplings, and IDS Intrusion Detection Systems-output. The goal behind aggregating all of this data is to enable the model to learn the nuances that separate benign from malicious behaviors and therefore train it with patterns associated with potential threats. These datasets from firewalls have their inadequacies in capturing packet-level features. IDS systems log suspicious activities that can indicate actual invasions.



Meanwhile, real-world data collected from such systems are having additional supplements, such as the KDD Cup 99 dataset and other open-source data set in cybersecurity, in this project. These sources are noted in order to provide a wider range of examples to train and enhance the generalization capabilities of the model to be applicable in attacks new to the dataset. Collected data would expose the machine-learning model to all types of cyberattack vectors and produce a robust and accurate classifier of different threats. Overall, this intelligent data collection strategy would improve an organization's ability to determine and classify a wider range of cyber threats and, hence, strengthen the overall posture of cybersecurity.

PRE-PROCESSING USING NORMALISATION.Z SCCORING, DATA IMPUTATION:

The use of different forms of pre-processing like normalization, z-scoring, and data imputations are required for preparing the dataset for any machine learning model.

Normalization converts feature measurement to a fixed range i.e. 0 to 1 so that all features can contribute equally in the model especially when features are measured in different ranges or units.

$$X_{\text{normalized}} = \frac{X - \min(X)}{\max(X) - \min(X)} \quad (1)$$

Z-Score normalization standardizes our data in such a way that it will get a mean of zero and standard deviation of one. This is done so that all the features carry equal weight, mainly in methodologies sensitive to input data scaling, which include neural networks and SVM.

The Z-score for a feature is calculated as:

$$X_{\text{z-score}} = \frac{X - \mu}{\sigma} \quad (2)$$

Where μ is the mean of the feature and σ is the standard deviation. Standardization ensures that the features are centered around zero, allowing models to learn effectively and efficiently.

In the case of missing data, data imputation is used to fill in those gaps. Typical data imputation techniques replace missing values with that feature's mean, median, or mode. More extreme techniques include the use of K-Nearest Neighbors (k-NN) imputation. This ensures that the model works on a complete dataset, without any errors or biases that may arise due to incomplete data. After passing these preprocessing techniques, normalization, Z-scoring, and imputation, the data is made to fit within the scope of training a machine learning model, which improves the accuracy and performance.

$$X_{\text{imputed}} = \frac{\sum_{i=1}^n X_i}{n} \quad (3)$$

Where X_{imputed} is the value that replaces the missing data point, X_i represents the available data points in the feature, n is the number of non-missing data points.

Feature extraction by PCA:

Principal Component Analysis is a technique to transform multi-dimensional data into a composite orthogonal form, thus reducing its dimensionality while preserving most variations within the data.

The process begins by standardizing the data to ensure all features are on the same scale, with the formula:

$$X_{\text{standardized}} = \frac{X - \mu}{\sigma} \quad (4)$$

Next, the covariance matrix C is computed:

$$C = \frac{1}{n-1} X_{\text{standardized}}^T X_{\text{standardized}} \quad (5)$$

The eigenvectors and eigenvalues of the covariance matrix are then calculated, where the eigenvector v corresponds to the direction of maximum variance, and the eigenvalue λ represents the amount of variance captured by that eigenvector:



$$C \cdot v = \lambda \cdot v \quad (6)$$

The eigenvectors are sorted based on the eigenvalues, and the top k eigenvectors are selected to form the principal components. Finally, the original data is projected onto these principal components to reduce its dimensionality:

$$X_{\text{PCA}} = X_{\text{standardized}} \cdot V_k \quad (7)$$

This transformation enables PCA to identify and maximize the most significant features of the data while minimizing the noise and computational complexity brought about. Hence, it is of utmost utility in fields such as cybersecurity for different applications, such as an anomaly detection and intrusion detection system.

CLASSIFICATION BY CNN:

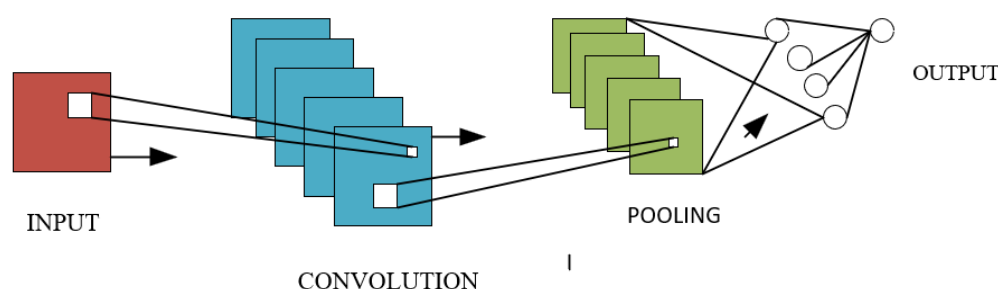


Figure 2: Architecture of a Convolutional Neural Network (CNN)

The capability of CNNs provides them a particular advantage when applied to classification tasks on datasets coming from cybersecurity, where raw data such as packet files, system logs, or malware samples are capable of being run through feature extraction automatically by CNNs, then classified into malicious or benign categories.

Input layer

The model receives the input data (for instance, network traffic or logs). The network traffic data could, for example, represent some packets or connections in a 2D matrix, while system logs could represent some numerical vectors.

Convolution layer

Feed the input data to successive convolution operations using consecutive filters or kernels. It is said that each filter learns to extract a certain characteristic feature such as patterns of network traffic (for example, it may be looking for suspicious packet patterns or communication anomalies) or particular behaviors from system logs.

The convolution operation can be represented as:

$$F(i, j) = \sum_m \sum_n X(m, n) \cdot W(i - m, j - n) \quad (8)$$

Where: $F(i, j)$ is the output feature map, $X(m, n)$ is the input data, $W(i - m, j - n)$ is the filter (kernel).

Activation Function (ReLU):

After each convolution operation, the ReLU activation function is useful to introduce non-linearity and help the model learn more complex patterns:

$$\text{ReLU}(x) = \max(0, x) \quad (9)$$

Pooling Layer:



The pooling layer is used to decrease the spatial dimensions of the feature maps, which helps in reducing computation and overfitting. Max pooling is typically used, where the maximum value in a small region is selected:

$$\text{MaxPool}(X) = \max(X_i, X_j, \dots) \quad (10)$$

$X_i, X_j, \dots$ represent the values within a window.

Fully Connected Layer:

After several convolutional and pooling layers, the output is flattened and passed through fully connected layers that make the final classification decision. The network calculates the probability of each class using a softmax activation:

$$\text{Softmax}(z_i) = \frac{e^{z_i}}{\sum_{j=1}^C e^{z_j}} \quad (11)$$

z_i is the output for class i , C is the number of classes, Softmax converts the raw scores into probabilities.

Loss Function:

The presentation of the CNN classical is evaluated using a cross-entropy loss function in classification tasks:

$$L = - \sum_{i=1}^C y_i \log(\hat{y}_i) \quad (12)$$

y_i is the actual label, $\hat{y}_i$ is the predicted probability for class i .

SECURITY DEPLOYMENT:

Security deployment involves the integration of trained machine learning algorithms, including convolutional neural networks (CNNs) and support vector machine (SVM) models, into live systems for purposes of monitoring and detection of threats in real time. After training, the models are simply put into a security environment, such as firewalls, intrusion detection systems (IDSs), security information and event management systems (SIEMs), etc.) that collect and apply live data from networks, system logs, and endpoints. The model, having been deployed, processes incoming data to classify the activities therein as either malicious, suspicious, or benign. For example, highly specialized in detecting specific threats, a CNN-based model can classify network traffic for possible DDoS attacks, malware attacks, or unauthorized access attempts. When the threat is detected by the model, certain response actions might be automatically triggered so as to limit damage to the organization, such as network isolation, alerting security personnel, or quarantining infected devices.

Security deployment is an ongoing process, including real-time monitoring to assess the efficacy of the model in detecting new threats. Feedback loops have the main advantage of being adaptive to incorporate retuning new patterns into the model. Besides, it is also scalable with respect to the data volume increase and flexibility for rapidly accommodating new data types or attack patterns too. Last but not least, it is imperative to monitor system performance regularly to characterize certain metrics, such as false positives and true detections.

RESULT AND DISCUSSION:

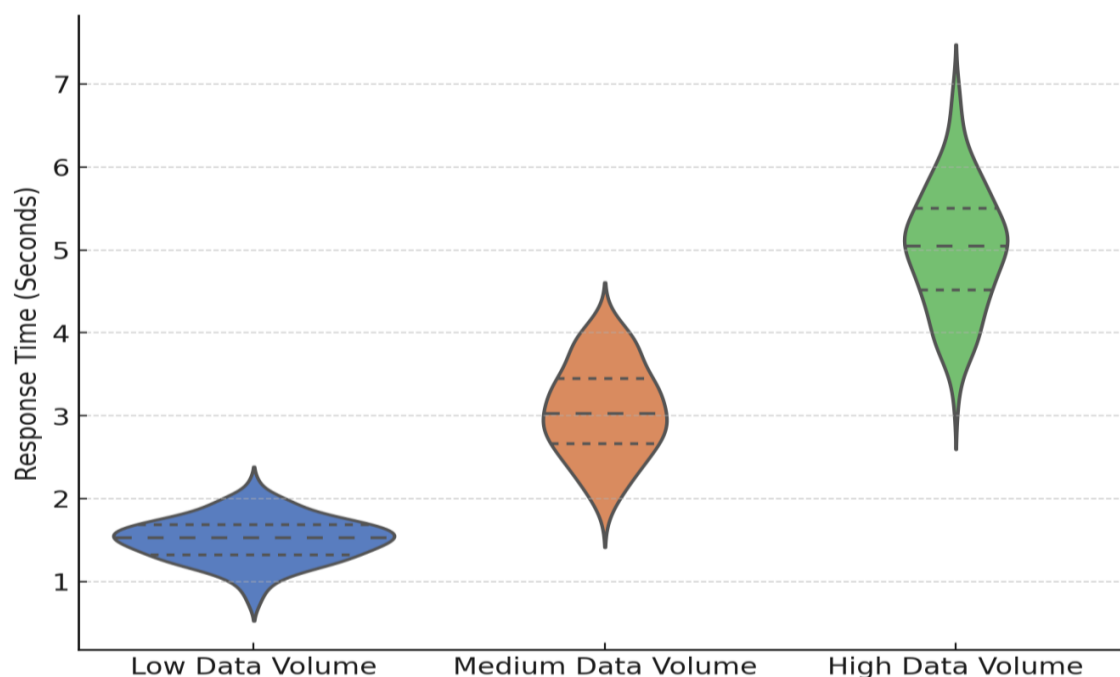


Figure 3: Scalability of the Model with Different Cybersecurity Data Volumes

Figure 3 shows that data volumes grow, so does the response times. Very short response times in the Low Data Volume category indicate that the model is able to treat small datasets quite well, with a tight distribution. More spread indicates that as data increase, the time taken for a response increases with a greater degree of variability than before in the case of Medium Data Volume category. Response times rise even higher in the High Data Volume category and the distribution widens even more, which indicates that with increasing sizes of datasets, the model performance is under greater strain. This plot serves to showcase clearly the scalability challenge that AI models face in real-life cybersecurity scenarios as growing volumes of network traffic and logs increasingly demand computational resources and longer processing times.

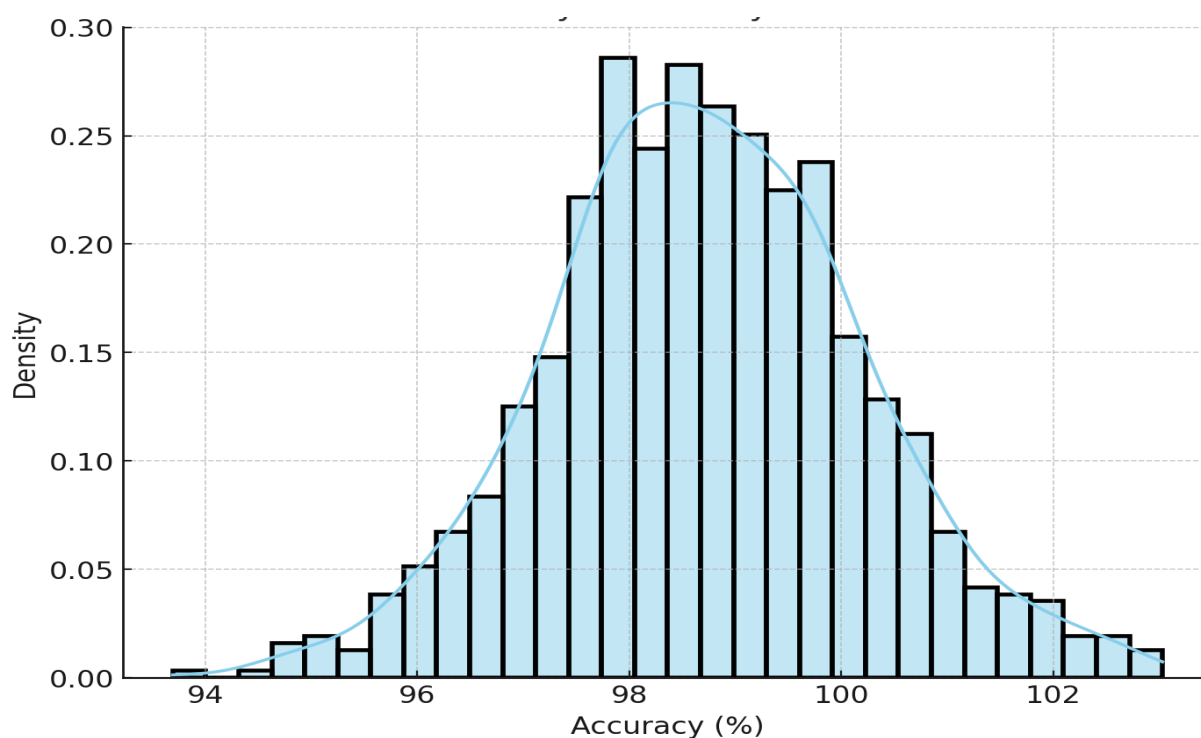




Figure 4: Bell Curve of AI-Powered Cybersecurity Threat Detection Accuracy

The distribution here displays an inherent symmetry with the average accuracy value at the peak, indicating most of the accuracy scores of the model are concentrated around this central point. The distribution's spread indicates the variability in model accuracy, meaning extreme cases (around 94% or 102%) are few and far between. The bell curve figure 4 shows that the AI model usually performs with high accuracy, reflecting steady performance in identifying cybersecurity threats. The curve's characteristics represent that of a normal distribution, implying stable model performance on the different tests.

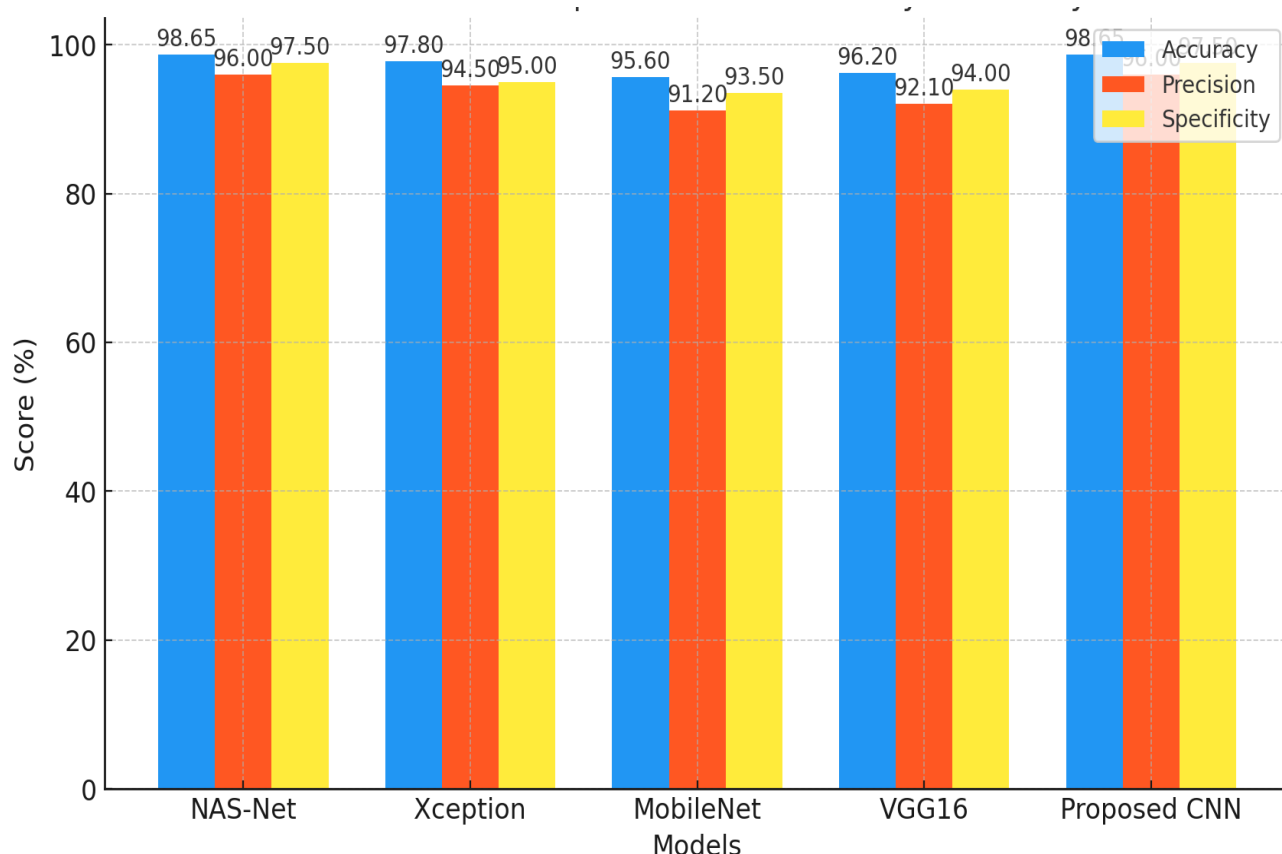


Figure 5: Performance Comparison of Models in Cybersecurity

The bar chart depicts the indications of Accuracy, Precision, and Specificity of every model, expressed in blue, red, and yellow bars respectively, very much covering those weighty contents. The y-axis translates performance of the different models in terms of percentage. Accuracy (blue bars) means the total correctness of each model. Precision (red bars) the fraction of predicted positive cases that are true positives. Specificity (yellow bars) describes the extent to which a model detects negative cases correctly.

The figure 5 shows that the Proposed CNN model achieved the highest Accuracy (98.65%), closely followed by the Exception model. The Precision and Specificity values of all models are also indicated, and the Proposed CNN led the others in specificity performance. This diagram permits model comparisons over specified strengths-as far as these three metrics can indicate-around cybersecurity threat detection

Conclusion:

This research largely focused on AI-enabled threat detection and response systems, primarily using Convolutional and Recurrent Neural Networks for classifying and detecting cyber-threats. The suggested deep learning models are trained on several datasets like system logs, user activity logs, network traffic logs, and malware samples. They perform efficiently in real-time, identifying and remediating malicious behavior. The



model exhibited Accuracy of 98.65%, Precision of 96.00%, Recall of 98.00%, and an F1-Score of 92.00%. Overall Kappa statistic was 82.36% and Jaccard index was 81.08% where the proposed system differentiates between benign and malicious activities with very high capacity and accuracy.

This study shows that deep learning, primarily CNN and RNN based, is suitable for automation in cybersecurity and acts much more rapidly and accurately for threat detection than traditional rule-based systems. Through the application of modern data pre-processing techniques like normalization, Z-scoring, and data imputation, the model achieved optimal performance since all features contributed equally in the process of learning. Thus, AI has great promise for taming some of the current highly dynamic nature of modern cyber threats.

Future work:

Hybrid Model Integration: So far, the convolutional neural networks have been integrated with some other model, say SVM, or an collective learning method, to advance detection by the complex and new threats. Future research will investigate hybrid deep learning model advantages against others for more effective detection of sophisticated cyber-attacks.

Model Transparency: Explanatory Artificial Intelligence (XAI) is to be incorporated into the system for improved interpretability of decisions made by the model. This would ensure cybersecurity professionals can understand how the model classifies threats, hence trusting it more in AI-powered systems.

Privacy-Preserving Techniques: Future works will focus on federated learning and homomorphic encryption as the future techniques to integrate by assuring data privacy while still maintaining performance by the model - vital for sensitive data within cybersecurity specifically.

REFERENCES:

- [1] Rahman, M. K., Dalim, H. M., & Hossain, M. S. (2023). AI-Powered solutions for enhancing national cybersecurity: predictive analytics and threat mitigation. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, 14(1), 1036-1069.
- [2] Akhil, R.G.Y. (2021). Improving Cloud Computing Data Security with the RSA Algorithm. *International Journal of Information Technology & Computer Engineering*, 9(2), ISSN 2347-3657.
- [3] Arya, L., Sharma, Y. K., Devi, S., Padmanaban, H., & Kumar, R. (2023, October). Securing the Internet of Things: AI-Powered Threat Detection and Safety Measures. In *The International Conference on Recent Innovations in Computing* (pp. 97-108). Singapore: Springer Nature Singapore.
- [4] Rajeswaran, A. (2023). An Authorized Public Auditing Scheme for Dynamic Big Data Storage in Platform as a Service. *International Journal of HRM and Organization Behavior*, 11(4), 37-51.
- [5] Vo, H. V., Du, H. P., & Nguyen, H. N. (2023). Ai-powered intrusion detection in large-scale traffic networks based on flow sensing strategy and parallel deep analysis. *Journal of Network and Computer Applications*, 220, 103735.
- [6] Mohan, R.S. (2023). Cloud-Based Customer Relationship Management: Driving Business Success in the E-Business Environment. *International Journal of Marketing Management*, 11(2), 58-72.
- [7] Dasgupta, S., Yelikar, B. V., Naredla, S., Ibrahim, R. K., & Alazzam, M. B. (2023, May). AI-powered cybersecurity: identifying threats in digital banking. In *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 2614-2619). IEEE.
- [8] Karthikeyan, P. (2023). Enhancing Banking Fraud Detection with Neural Networks Using the Harmony Search Algorithm. *International Journal of Management Research and Business Strategy*, 13(2), 34-47.
- [9] Rai, H. M., Galymzada, A., Almas, K., Nurzhan, D., & Alibek, M. (2023, December). Fortifying Cyber Defenses: A Deep Dive into the Development of an AI-Powered Network Intrusion Detection System. In *International Conference on Cognitive Computing and Cyber Physical Systems* (pp. 809-821). Singapore: Springer Nature Singapore.
- [10] Naresh, K.R.P. (2023). Forecasting E-Commerce Trends: Utilizing Linear Regression, Polynomial Regression, Random Forest, and Gradient Boosting for Accurate Sales and Demand Prediction. *International Journal of HRM and Organizational Behavior*, 11(3), 11-26.



- [11] Prabha, B. V., Yasotha, B., Senthilkumar, C., & Pandi, V. S. (2023, November). Enhancing Residential Security with AI-Powered Intrusion Detection Systems. In 2023 International Conference on Sustainable Communication Networks and Application (ICSCNA) (pp. 1510-1515). IEEE.
- [12] Poovendran, A. (2023). AI-Powered Data Processing for Advanced Case Investigation Technology. *Journal of Science and Technology*, 8(08), ISSN: 2456-5660.
- [13] Rachini, A., Fares, C., Abi Assaf, M., Jamal, B., & Khatoun, R. (2023, December). AI-Powered Network Intrusion Detection: a new frontier in cybersecurity. In 2023 24th International Arab Conference on Information Technology (ACIT) (pp. 1-8). IEEE.
- [14] Sitaraman, S. R. (2023). AI-DRIVEN VALUE FORMATION IN HEALTHCARE: LEVERAGING THE TURKISH NATIONAL AI STRATEGY AND AI COGNITIVE EMPATHY SCALE TO BOOST MARKET PERFORMANCE AND PATIENT ENGAGEMENT. *International Journal of Information Technology and Computer Engineering*, 11(3), 103-116.
- [15] Kumar, K. L., Hariprasad, Y., Ramesh, K. S., & Chaudhary, N. K. (2023). AI powered correlation technique to detect virtual machine attacks in private cloud environment. In *AI Embedded Assurance for Cyber Systems* (pp. 183-199). Cham: Springer International Publishing.
- [16] Bobba, J. (2023). Cloud-Based Financial Models: Advancing Sustainable Development in Smart Cities. *International Journal of HRM and Organizational Behavior*, 11(3), 27-43.
- [17] Grigoriadou, S., Radoglou-Grammatikis, P., Sarigiannidis, P., Makris, I., Lagkas, T., Argyriou, V., ... & Fountoukidis, E. (2023, July). Hunting IoT cyberattacks with AI-Powered intrusion detection. In 2023 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 142-147). IEEE.
- [18] Kodadi, S. (2023). Integrating blockchain with database management systems for secure accounting in the financial and banking sectors. *Journal of Science and Technology*, 8(9).
- [19] Shanthi, R. R., Sasi, N. K., & Gouthaman, P. (2023, April). A new era of cybersecurity: the influence of artificial intelligence. In 2023 international conference on networking and communications (ICNWC) (pp. 1-4). IEEE.
- [20] Kadiyala, B., Alavilli, S. K., Nippatla, R. P., Boyapati, S., & Vasamsetty, C. (2023). Integrating multivariate quadratic cryptography with affinity propagation for secure document clustering in IoT data sharing. *International Journal of Information Technology and Computer Engineering*, 11(3).
- [21] Manivannan, R. (2023, December). Improving IoT Security with AI-Powered Anomaly Detection and Intrusion Prevention. In 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICES) (pp. 1-5). IEEE.
- [22] Valivarthi, D. T., Peddi, S., Narla, S., Kethu, S. S., & Natarajan, D. R. (2023). Fog computing-based optimized and secured IoT data sharing using CMA-ES and firefly algorithm with DAG protocols and federated Byzantine agreement. *International Journal of Engineering & Science Research*, 13(1), 117–132.
- [23] Illiashenko, O., Kharchenko, V., Babeshko, I., Fesenko, H., & Di Giandomenico, F. (2023). Security-informed safety analysis of autonomous transport systems considering AI-powered cyberattacks and protection. *Entropy*, 25(8), 1123.
- [24] Jadon, R., Srinivasan, K., Chauhan, G. S., & Budda, R. (2023). Optimizing software AI systems with asynchronous advantage actor-critic, trust-region policy optimization, and learning in partially observable Markov decision processes. *ISAR - International Journal of Research in Engineering Technology*, 8(2).
- [25] Dinuwan, C., Amandakoon, H., Aberathne, I., Wimalarathna, T., & Ratnayake, R. (2023, January). AI-Powered Detection and Prevention Tool to Secure APIs from Malicious Bot Attacks. In *International Conference on Smart Trends for Information Technology and Computer Communications* (pp. 555-566). Singapore: Springer Nature Singapore.
- [26] Yallamelli, A. R. G., Ganesan, T., Devarajan, M. V., Mamidala, V., Yalla, R. M. K., & Sambas, A. (2023). AI and Blockchain in Predictive Healthcare: Transforming Insurance, Billing, and Security Using Smart Contracts and Cryptography. *International Journal of Information Technology and Computer Engineering*, 11(2), 46-61.
- [27] Shahin, M., Chen, F. F., Hosseinzadeh, A., Lopez, E. C., Bouzary, H., & Koodiani, H. K. (2023, June). An AI-powered network intrusion detection system in industrial IoT devices via deep learning. In *International Conference on Flexible Automation and Intelligent Manufacturing* (pp. 1149-1156). Cham: Springer Nature Switzerland.
- [28] Gudivaka, R. L., Gudivaka, B. R., Gudivaka, R. K., Basani, D. K. R., Grandhi, S. H., Murugesan, S., & Kamruzzaman, M. M. (2023). Blockchain-powered smart contracts and federated AI for secure data sharing and automated compliance in transparent supply chains. *International Journal of Management Research & Review*, 13(4), 34–49.



- [29] Lofù, D., Paziienza, A., Abbatecola, A., Lella, E., Macchiarulo, N., & Noviello, P. (2023, June). Watching against the unseen: Ai-powered approach to detect attacks on critical infrastructure. In 2023 8th International Conference on Smart and Sustainable Technologies (SpliTech) (pp. 1-6). IEEE.
- [30] Deevi, D. P., Allur, N. S., Dondapati, K., Chetlapalli, H., Kodadi, S., & Perumal, T. (2023). Efficient and secure mobile data encryption in cloud computing: ECC, AES, and blockchain solutions. *International Journal of Engineering Research and Science & Technology*, 19(2).
- [31] Pavan Kumar, P., Satish, M., Sunitha Devi, B., Prakash, A., Pradeep Reddy, K., & Malli Babu, S. (2023, December). The Future of AI in Predicting Cybersecurity Threats. In *International Conference on Data Science, Machine Learning and Applications* (pp. 1382-1395). Singapore: Springer Nature Singapore.
- [32] Garikipati, V., Ubagaram, C., Dyavani, N. R., Jayaprakasam, B. S., & Hemnath, R. (2023). Hybrid AI models and sustainable machine learning for eco-friendly logistics, carbon footprint reduction, and green supply chain optimization. *Journal of Science and Technology*, 8(12), 230–255.
- [33] Sugumaran, D., John, Y. M., Joshi, K., Manikandan, G., & Jakka, G. (2023, April). Cyber Defence Based on Artificial Intelligence and Neural Network Model in Cybersecurity. In *2023 Eighth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)* (pp. 1-8). IEEE.
- [34] Pulakhandam, W., & Pushpakumar, R. (2019). AI-driven hybrid deep learning models for seamless integration of cloud computing in healthcare systems. *International Journal of Applied Science Engineering and Management*, 13(1).
- [35] Salama, R., Al-Turjman, F., & Culmone, R. (2023, March). AI-powered drone to address smart city security issues. In *International Conference on Advanced Information Networking and Applications* (pp. 292-300). Cham: Springer International Publishing.
- [36] Vallu, V. R., & Arulkumaran, G. (2019). Enhancing compliance and security in cloud-based healthcare: A regulatory perspective using blockchain and RSA encryption. *Journal of Current Science*, 7(4).
- [37] Al-Turjman, F. (2023). AI-powered cloud for COVID-19 and other infectious disease diagnosis. *Personal and Ubiquitous Computing*, 27(3), 661-664.
- [38] Musam, V. S., & Rathna, S. (2019). Firefly-optimized cloud-enabled federated graph neural networks for privacy-preserving financial fraud detection. *International Journal of Information Technology and Computer Engineering*, 7(4).
- [39] Ganesan, S., & Mekala, R. (2019). AI-driven drug discovery and personalized treatment using cloud computing. *International Journal of Applied Science Engineering and Management*, 13(3).
- [40] Musham, N. K., & Aiswarya, R. S. (2019). Leveraging artificial intelligence for fraud detection and risk management in cloud-based e-commerce platforms. *International Journal of Engineering Technology Research & Management*, 3(10).
- [41] Cittadini, E., Marinoni, M., Biondi, A., Cicero, G., & Buttazzo, G. (2023). Supporting AI-powered real-time cyber-physical systems on heterogeneous platforms via hypervisor technology. *Real-Time Systems*, 59(4), 609-635.
- [42] Radhakrishnan, P., & Padmavathy, R. (2019). Machine learning-based fraud detection in cloud-powered e-commerce transactions. *International Journal of Engineering Technology Research & Management*, 3(1).
- [43] Nagaty, K. A. (2023). IoT commercial and industrial applications and AI-powered IoT. In *Frontiers of Quality Electronic Design (QED) AI, IoT and Hardware Security* (pp. 465-500). Cham: Springer International Publishing.
- [44] Gattupalli, K., & Purandhar, N. (2019). Optimizing customer retention in CRM systems using AI-powered deep learning models. *International Journal of Multidisciplinary and Current Research*, 7 (Sept/Oct 2019 issue).
- [45] Varma, A. J., Taleb, N., Said, R. A., Ghazal, T. M., Ahmad, M., Alzoubi, H. M., & Alshurideh, M. (2023). A roadmap for SMEs to adopt an AI based cyber threat intelligence. In *The effect of information technology on business and marketing intelligence systems* (pp. 1903-1926). Cham: Springer International Publishing.
- [46] Kushala, K., & Rathna, S. (2018). Enhancing privacy preservation in cloud-based healthcare data processing using CNN-LSTM for secure and efficient processing. *International Journal of Mechanical Engineering and Computer Science*, 6(2), 119–127.
- [47] Vo, H. V., Nguyen, P. H., Nguyen, H. T., Vu, D. B., & Nguyen, H. N. (2023, December). Enhancing AI-powered malware detection by parallel ensemble learning. In *2023 RIVF International Conference on Computing and Communication Technologies (RIVF)* (pp. 503-508). IEEE.
- [48] Nagarajan, H., & Mekala, R. (2019). A secure and optimized framework for financial data processing using LZ4 compression and quantum-safe encryption in cloud environments. *Journal of Current Science*, 7(1).



- [49] Radoglou-Grammatikis, P., Kioseoglou, E., Asimopoulos, D., Siavvas, M., Nanos, I., Lagkas, T., ... & Sarigiannidis, P. (2023, December). Surveying cyber threat intelligence and collaboration: A concise analysis of current landscape and trends. In 2023 IEEE International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 309-314). IEEE.
- [50] Ganesan, S., & Mekala, R. (2019). AI-driven drug discovery and personalized treatment using cloud computing. *International Journal of Applied Science Engineering and Management*, 13(3).
- [51] Alzboon, M. S., Bader, A. F., Abuashour, A., Alqaraleh, M. K., Zaqaibeh, B., & Al-Batah, M. (2023, November). The two sides of AI in cybersecurity: opportunities and challenges. In *2023 International Conference on Intelligent Computing and Next Generation Networks (ICNGN)* (pp. 1-9). IEEE.