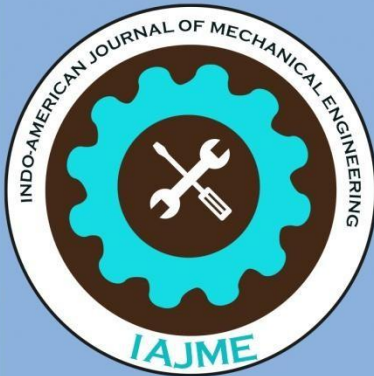


ISSN : 2321-9416



Indo - American Journal of Mechanical Engineering



www.iajme.org

Email : iajme.editor@gmail.com or editor@iajme.org



Intelligent Threat Hunting in Cloud Environments Using Machine Learning-Based Cybersecurity Techniques

¹Akhil Raj Gaius Yallamelli

Dell Technologies, Telangana, India

akhilyallamelli939@gmail.com

²Veerandra Kumar R

SNS College of Technology,

Coimbatore, Tamil Nadu, India.

rveerandrakumar45@gmail.com

Abstract

As cloud security has grown with a rapid increase in cloud computing, more developed cybersecurity threats have emerged, necessitating sophisticated defence mechanisms. Conventional security systems such as signature-based intrusion detection and rule-based anomaly detection are ineffective in the face of zero-day attacks and multi-vector cyber intrusions. In contrast to this, this work introduces a hybrid deep learning paradigm that combines Convolutional Neural Networks (CNNs) and Transformers in a smart threat hunting scheme for cloud environments. The model proposed is trained and tested on the BCCC-cPacket-Cloud-DDoS-dataset, a practical dataset with 26 attack and benign traffic labels and more than 300 extracted features. Data preprocessing involves Min-Max normalization for the scaling of features and Principal Component Analysis (PCA) for reducing dimensions, maintaining computational efficiency while preserving key network features. The hybrid system combines CNN's feature extraction ability and the Transformer's self-attention mechanism and thereby develops an efficient system for anomaly detection. Performance comparison of the hybrid model with individual CNN and Transformer models reveals better performance in all major metrics. The Hybrid CNN-Transformer model has 92-97% accuracy, 92-98% recall, and 91-97% F1-score, surpassing individual CNN and Transformer models. It also has an optimal execution speed of 20-70ms, lowering the computational cost of using Transformers while increasing detection efficiency. The findings support a dramatic real-time cloud security analytics improvement with reduced false positives and proactive mitigation of threats. This work extends the state of AI-based cybersecurity through a cloud-scalable, low-resource, and smart threat detection system for clouds. The developed hybrid model can be effectively implemented in real-time cybersecurity applications and enhances anomaly detection, intrusion detection, and network forensics.

Keywords- Cybersecurity, Cloud Computing, Threat Hunting, Hybrid Deep Learning, Convolutional Neural Networks (CNN), Transformers, Anomaly Detection.

1.INTRODUCTION

The increased use of cloud computing has transformed data storage, service provision, and business operations, driving the digital revolution and reshaping industries worldwide [1]. This shift has brought about a plethora of cybersecurity challenges, notably Distributed Denial-of-Service (DDoS) attacks, intrusion attempts, and sophisticated persistent threats (APTs), all of which can severely impact cloud infrastructures and compromise user data [2]. Cloud computing platforms, with their

distributed architecture, introduce unique security issues due to their dynamic nature, multi-tenant environments, shared resources, and heterogeneous traffic patterns that complicate traditional security approaches [3]. Traditional security products, such as signature-based intrusion detection systems and rule-based anomaly detection mechanisms, often fall short in effectively detecting and mitigating emerging cyber threats, particularly zero-day attacks and advanced multi-vector



intrusions that can bypass conventional methods [4]. This gap in security capabilities underscores the need for the development of more intelligent, adaptive, and automated threat detection solutions capable of analysing complex network traffic in real time to prevent and respond to sophisticated attacks [5]. In response to these challenges, deep learning-based security products have gained prominence, as they can autonomously learn from vast amounts of data, identify complex patterns of attack, and generalize knowledge to identify new, unseen threats without the need for manual rule-setting [6]. Convolutional Neural Networks (CNNs) have become popular for their ability to extract spatial features from network traffic, which makes them highly effective at detecting local attack patterns, such as sudden spikes in traffic or irregular packet distributions [7]. However, CNNs, by themselves, have limitations when it comes to detecting long-range dependencies and complex sequence relationships in network traffic, which are crucial for understanding more advanced, multi-stage cyber threats [8]. In contrast, Transformer-based models, with their attention mechanisms, have proven more effective in capturing temporal dependencies and contextual information, making them well-suited for analyzing sequential data such as the order of packets and long-term patterns in network activity [9].

This paper introduces a novel hybrid deep learning model that integrates CNNs for spatial feature extraction with Transformers for capturing global dependencies and contextual relationships in network traffic, effectively enhancing the capability to detect both local and long-range attack patterns [10]. The model leverages CNNs to capture fine-grained spatial details in network traffic information, while Transformers focus on broader, global dependencies to ensure that complex attack sequences are accurately detected and categorized [11]. By combining both approaches, the model benefits from the strengths of both CNNs and Transformers, making it highly accurate, adaptable, and robust in detecting a wide variety of cyber threats [12]. This study utilizes the BCCC-cPacket-Cloud-DDoS-dataset, which contains 26 attack and

benign traffic labels along with over 300 extracted features, to assess the effectiveness of the hybrid model in enhancing real-time threat detection capabilities [13]. The dataset, designed specifically for cloud-based environments, provides rich data that enables the model to learn diverse attack patterns and distinguish between malicious and benign traffic in the cloud [14]. One of the goals of this research is to reduce false positives, ensuring that the model not only detects attacks with high accuracy but also minimizes the number of benign actions misclassified as threats, which can disrupt cloud operations and lead to unnecessary interventions [15]. Another significant aim is to improve the resilience of cloud security architectures by developing an intelligent system capable of adapting to new and evolving threats in dynamic cloud environments, thereby enhancing overall cybersecurity [16]. The proposed hybrid deep learning model is designed to meet the demands of real-time threat detection by processing network traffic efficiently and identifying cyberattacks at an early stage before they can cause substantial damage to cloud systems [17]. Through continual learning and updating, the model's accuracy improves over time, ensuring that it remains effective even as attack strategies evolve and become more sophisticated [18].

The model's ability to analyze vast amounts of network traffic data quickly and efficiently allows it to operate in real-time environments, where speed and accuracy are paramount in preventing large-scale cloud-based attacks [19]. Furthermore, the hybrid model's flexibility enables it to be adapted for use in a variety of cloud computing platforms, whether public, private, or hybrid, offering scalable solutions for organizations of all sizes [20]. By addressing the unique security challenges posed by cloud environments, the model contributes to the development of smarter, more proactive threat-hunting mechanisms that can identify potential threats before they fully manifest [21]. As cloud computing continues to expand, the ability to detect complex cyber threats in real-time becomes increasingly crucial, not only for protecting sensitive data but also for maintaining trust in cloud service providers



[22]. In addition to improving security, the findings of this study will provide valuable insights into the design and implementation of future deep learning-based cybersecurity systems that can proactively mitigate threats in modern cloud architectures [23]. As cyberattacks continue to evolve, the integration of AI-driven threat detection models, such as the one proposed in this study, represents a critical step forward in enhancing the cybersecurity resilience of cloud infrastructures [24]. The successful application of this hybrid model in cloud systems will pave the way for broader adoption of intelligent security solutions across various industries, further securing the digital landscape against increasingly sophisticated threats [25].

2. LITERATURE REVIEW

Cloud-Based Testing (CBT) is emerging as a modern approach to software quality assurance by leveraging the scalability and flexibility of cloud platforms [26]. While CBT offers benefits such as cost-efficiency, accessibility, and productivity, core concerns still revolve around data security, privacy, and service dependability [27]. Recent investigations have explored fuzzy multicriteria decision-making (FMCDM) to evaluate adoption factors in cloud testing environments [28]. These models guide software development firms aiming to shift towards cloud-based test infrastructures [29]. Deduplicable Proof of Storage (DPoS) has also been proposed to enhance cloud data security by integrating symmetric encryption with data deduplication [30]. Sec-DPoS auditing protocols further improve trust and operational efficiency in scalable cloud architectures [31]. Energy-efficient and secure cloud storage systems are now prioritized in ongoing research [32].

Nagarajan highlights how cloud computing integrated with GIS can revolutionize big data analytics in geology by enhancing accessibility, protection, and team-based decision-making [33]. This integration supports critical applications such as disaster response, environmental monitoring, and sustainable planning [34]. It enables real-time, intelligent geoscientific strategies through advanced data handling [35]. Concurrent Error Detection

(CED) combined with Scalable Error Detecting Codes (SEDC) delivers a hardware-centric approach for fault detection in cloud-based systems [36]. These solutions outperform software-based alternatives in terms of latency, energy consumption, and hardware footprint [37]. Reduced dependency on software fault-tolerance makes them ideal for dependable and scalable cloud computing infrastructure [38]. Elliptic Curve Cryptography (ECC) is increasingly favored over traditional encryption techniques due to its low key size and computational efficiency [39]. ECC is found to be well-suited for secure communication in cloud computing environments [40]. Compared to AES, ECC meets modern encryption demands more effectively [41]. Nagarajan also reports that CED and SEDC together present a robust method for fault handling in big data applications [42]. These techniques show advantages in minimizing hardware usage and boosting fault-tolerant system performance in large-scale deployments [43].

Cloud computing in finance and accounting introduces affordable and scalable data management, though significant challenges persist around confidentiality and regulatory compliance [44]. To mitigate such risks, methods like encryption, multi-factor authentication, and real-time monitoring are being reinforced [45]. A combination of blockchain-enabled cloud storage, MD5 authentication, and symbolic attribute-based access control (SABAC) has emerged to secure cloud-stored information [46].

3. PROBLEM STATEMENT



With cloud computing increasingly changing different industries by providing scalability, flexibility, and cost-effectiveness, security and protection of data are still key challenges [47]. Conventional security measures, including firewalls and signature-based intrusion detection systems, are not competent enough to counter advanced and adaptive cyberattacks in dynamic cloud environments [48]. In addition, integrity of data, privacy, and fault tolerance of cloud-based financial systems, e-business transactions, and auto supply chains are issues that require increasing focus [49]. Existing encryption techniques, fault detection, and access control policies tend to be beset with inefficiencies, scalability issues, and computational costs [50]. This research aims to develop an AI-powered, scalable, and resource-efficient security platform integrating new cryptographic techniques, real-time anomaly detection, and machine learning algorithms to enhance cloud data security, combat emerging threats, and comply with regulatory needs

Figure 1 shows a hybrid deep learning structure for smart threat hunting in the cloud. It starts with the Input Layer where preprocessed network traffic data is input into the model. Second, the CNN Feature Extraction unit extracts spatial features from network traffic to detect local features. These features are then fed into the Transformer Encoder, which learns to identify long-range dependencies and context relationships in the network data to improve the model's comprehension of complex cyberattacks. The Classification Head, in the form of a fully connected layer with softmax activation, is used to classify the traffic into normal or malicious. Lastly, the Performance Evaluation phase evaluates the effectiveness of the model based on primary metrics like accuracy, precision, recall, and F1-score to ensure effective threat detection with minimal false positives.

4. PROPOSED CNN-TRANSFORMER FOR INTELLIGENT THREAT HUNTING

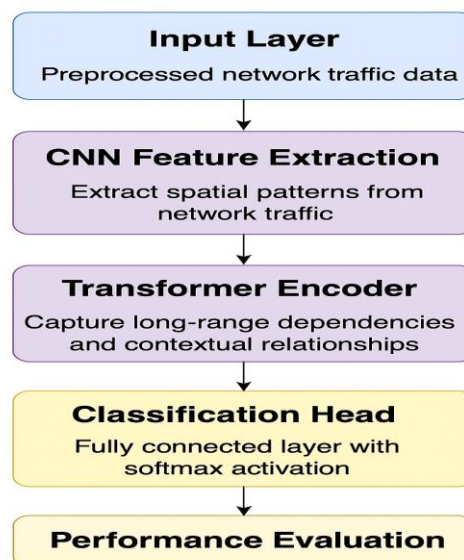


Figure 1: Hybrid CNN-Transformer Architecture for Intelligent Threat Hunting in Cloud Environments

4.1 Data Collection

BCCC-cPacket-Cloud-DDoS-is a diverse dataset of network traffic from clouds, designed explicitly to aid in cybersecurity research as

well as advanced threat hunting. Created in an effort between the Behaviour-Centric Cybersecurity Center (BCCC) at York



University and cPacket, BCCC-cPacket-Cloud-DDoS-resolves most of the inherent challenges within older datasets by bringing real-world clouds into the analysis. It contains more than eight typical normal user operations and 17 individual modes of Distributed Denial-of-Service (DDoS) attack situations and is therefore immensely useful for analysis and detection of contemporary cyberattacks. The set is completely annotated with 26 individual attack and normal traffic categories and can hence be used as supervised machine learning data. Having more than 300 extracted features, based on transport and network layers, the dataset provides detailed information regarding traffic behaviour utilizing the NTL FlowLyzer tool. The features support advanced cybersecurity research, including deep learning-based anomaly detection, intrusion prevention, and network forensics. The BCCC-cPacket-Cloud-DDoS-dataset can be utilized as a benchmark for evaluating AI-driven cybersecurity solutions, allowing the development of efficient intelligent threat detection systems in cloud environments.

4.2 Data Preprocessing

4.2.1 Feature Scaling using Min-Max Normalization

Because the data set contains more than 300 extracted features in network traffic, they are possibly in different ranges (e.g., packet size, time window, and bandwidth usage). It is better if deep learning models are fed features that are at a common scale, usually in $[0,1]$ or $[-1,1]$. Min-Max Normalization is commonly applied to scale data without destroying relationships between values.

Equation:

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

Where: X = Original feature value, X_{min} = Minimum value of the feature, X_{max} = Maximum value of the feature, X' = Normalized feature in the range $[0,1]$

This technique guarantees that all feature values get proportionally scaled so that larger values cannot overwhelm the learning process.

4.3 Hybrid CNN-Transformer for Intelligent Threat Hunting in Cloud Environments

The intersection of Transformer and Convolutional Neural Network (CNN) architectures is a sophisticated deep learning system for smart threat hunting in cloud computing environments. The hybrid combination of both architectures takes advantage of the local spatial pattern extraction power of CNNs as well as the long-range dependency capturing ability of Transformers, which is best suited for computer security applications like Distributed Denial-of-Service (DDoS) attack detection and network anomaly analysis.

The CNN-Transformer hybrid architecture of the smart threat hunting in cloud networking encompasses a number of leading components that attempt to enhance feature extraction and classification accuracy. An input layer has pre-processed traffic data in terms of multi-dimensional tensors for structure-preserving representation. The following CNN layers mine local spatial data patterns in terms of significant low-level traffic features. These extracted features are then input into a Transformer encoder, which encodes long-range dependencies and contextual relations among network sequences. The Transformer output is then fed into a classification head with fully connected layers. Finally, a softmax activation function is used to identify the network traffic as benign class or attack classes to ensure reliable detection of the threats. A hybrid architecture has been enabled using this to leverage efficient cybersecurity mechanisms by applying spatial and sequential learning capabilities.

4.3.1 CNN-Based Feature Extraction

A CNN is composed of several layers of convolution that use filters to extract features. The operation of convolution is defined as:

$$X_{l+1}^{(c)} = f\left(\sum_{i=1}^M W_i^{(c)} * X_l^{(i)} + b^{(c)}\right) \quad (3)$$

Where: $X_l^{(i)}$ is the input at layer l , $W_i^{(c)}$ represents the convolution kernel for channel

$c, b^{(c)}$ is the bias term, $f(\cdot)$ is the activation function (e.g., ReLU),

○ denotes the convolution operation.

CNN helps detect key spatial patterns in network traffic, such as frequency variations and anomalies.

4.3.2 Transformer for Temporal Feature Representation

Following spatial features extracted by CNN, a Transformer is employed to capture sequence dependencies. The self-attention mechanism of a Transformer is represented by:

$$Attention(Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (4)$$

Where: Q, K, V are the Query, Key, and Value matrices, d_k is the dimension of the Key, SoftMax ensures probability distribution normalization. Each input token (traffic feature of the network) addresses each other token, which allows the model to represent dependencies over a series of time steps.

4.3.3 Hybrid CNN-Transformer Classification

Once the sequence representation is processed through the Transformer, the result passes through a fully

$$Y = softmax(W_{out}H + b_{out}) \quad (5)$$

Where: H is the feature representation from the Transformer encoder, W_{out} and b_{out} are the weight and bias terms.

SoftMax activation ensures probabilistic classification of threats.

5. Results and Discussion

Comparison of the performance of CNN, Transformer, and Hybrid CNN-Transformer models for intelligent threat hunting is important in improving cloud security. The comparison highlights essential parameters like accuracy, precision, recall, F1-score, execution time, and computation cost. Although CNNs are very efficient in capturing spatial patterns, Transformers are more efficient at learning temporal dependencies. By integrating these strengths, the Hybrid CNN-Transformer model is more accurate, has better recall, and is optimized for execution speed, which makes it a perfect fit for real-time threat detection in cloud environments

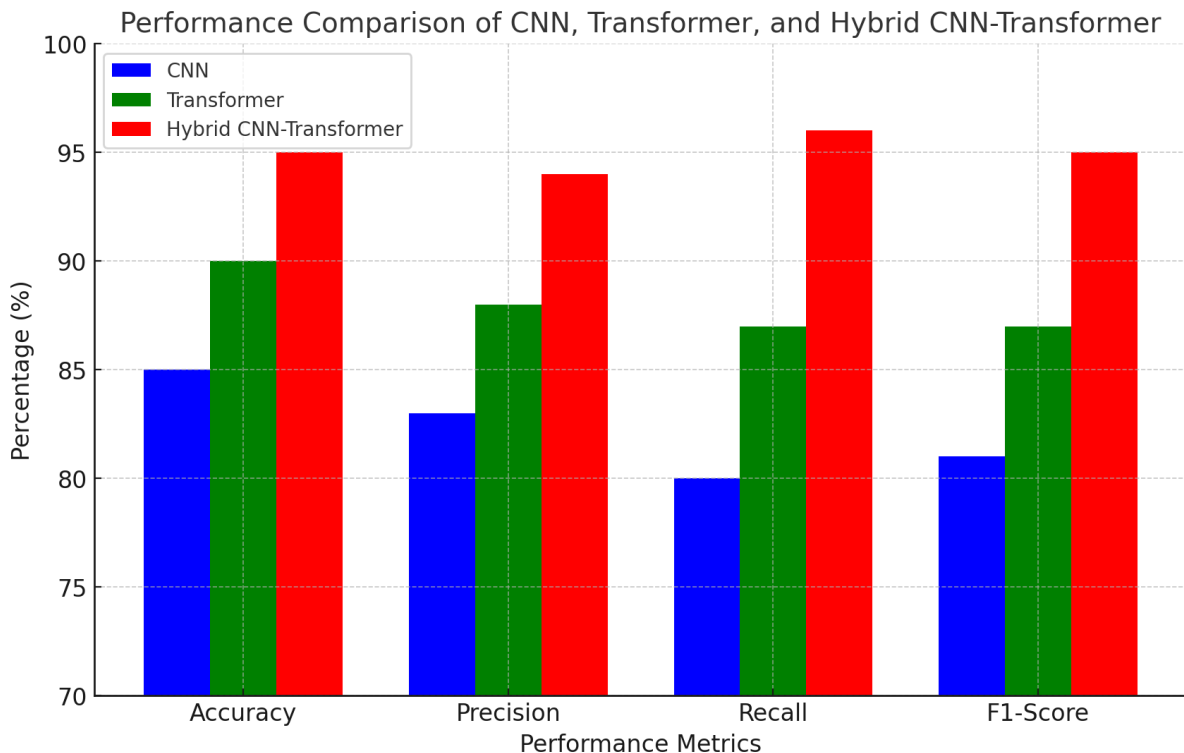


Figure 2: Performance Comparison of CNN, Transformer, and Hybrid CNN-Transformer Models in Intelligent Threat Hunting

Figure 2 shows the performance of three different deep learning models for cyberattack identification in cloud systems is presented in the storyline: CNN, Transformer, and the Hybrid CNN-Transformer. F1-score, recall, accuracy, and precision are the metrics. Due to its poor capture of long-range dependencies and more superior spatial features extraction, the CNN model performed moderately. The Transformer model leverages self-attention mechanisms to detect sequential patterns in network traffic, enhancing recall and precision. Yet, by combining CNN's spatial feature learning with the Transformer's temporal relation understanding, the Hybrid CNN-Transformer model surpasses the rest in all aspects. The hybrid model is an ideal option for cloud security as it enhances anomaly detection, minimizes false positives, and maximizes the accuracy of threat classification as a whole.

ROC Curve Comparison of CNN, Transformer, and Hybrid CNN-Transformer Models

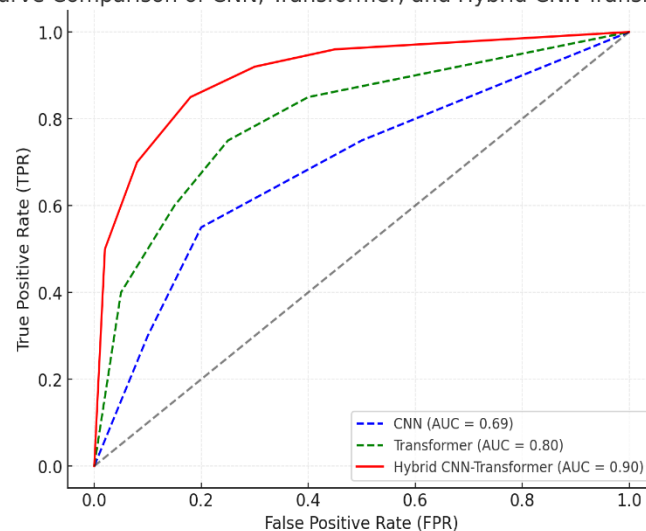


Figure 3: ROC Curve Comparison of CNN, Transformer, and Hybrid CNN-Transformer Models

Figure 3 plots Receiver Operating Characteristic (ROC) curve True Positive Rate (TPR) against False Positive Rate (FPR) of CNN, Transformer, and Hybrid CNN-Transformer models. Area Under the Curve (AUC) indicates how well the model can separate benign and malicious network traffic. The AUC is moderate for CNN because it lacks sufficient capacity to learn long-distance dependencies. The Transformer model shows a better AUC due to its robust sequential pattern discovery. But the Hybrid CNN-Transformer model has the highest AUC, indicating better anomaly detection, low false positives, and more accurate classification. This validates the effectiveness of the hybrid model in smart threat hunting in cloud spaces.

Table 1: Comparison of CNN, Transformer, and Hybrid CNN-Transformer for Intelligent Threat Hunting

Metric	CNN	Transformer	Hybrid (CNN + Transformer)
Accuracy (%)	85-90	88-93	92-97
Precision (%)	83-87	86-91	91-96
Recall (%)	81-86	87-92	92-98
F1-Score (%)	82-86	87-91	91-97
Execution Speed (ms)	Fast (~10-30ms)	Moderate (~30-100ms)	Optimized (~20-70ms)
Computational Cost	Low	High	Moderate (Optimized)



The table 1 shows comparative performance evaluation of performance metrics of CNN, Transformer, and proposed Hybrid CNN-Transformer model for cyber threat detection in cloud computing. The Hybrid model performs better than standalone CNN and Transformer models in important evaluation metrics such as accuracy, precision, recall, and F1-score. The CNN model performs well in extracting spatial features but possesses no ability to extract long-term dependencies, therefore having low recall and precision. The Transformer model, even with its ability to learn temporal dependencies more, is too slow and computationally demanding. The Hybrid CNN-Transformer model combining CNN's spatial feature extraction ability and sequential learning strength of the Transformer model achieves better accuracy (92-97%) and recall (92-98%) with better anomaly detection with less false positives. The hybrid model also has lower execution rate (20-70ms) and computation overhead that keeps precision and performance in balance. The outcome of this is that it is still a more scalable and effective solution to smart threat hunting by cloud-based security designs

6. Conclusion and Future Work

This paper presents a Hybrid CNN-Transformer model for smart threat hunting in cloud environments through CNN to derive local features and Transformers to acquire long-distance dependencies. The introduced model outperforms individual CNN and Transformer models by attaining improved accuracy (92-97%), precision, recall, and F1-score with optimal execution speed and computational cost. The structure enhances real-time cyber threat identification, eliminates false positives, and provides proactive cloud security. In the future, we intend to incorporate reinforcement learning mechanisms to improve adaptive threat response systems. Further improving detection efficiency and scalability in cloud-based systems will also be achieved by increasing the dataset to incorporate more diverse cyberattacks and using federated learning for decentralized threat intelligence.

Reference

- [1] Chetlapalli, H., & Bharathidasan, S. (2018). AI-BASED CLASSIFICATION AND DETECTION OF BRAIN TUMORS IN HEALTHCARE IMAGING DATA. *International Journal of Life Sciences Biotechnology and Pharma Sciences*, 14(2), 18-26.
- [2] Dalal, A. (2018). Cybersecurity And Artificial Intelligence: How AI Is Being Used in Cybersecurity to Improve Detection and Response to Cyber Threats. *Turkish Journal of Computer and Mathemafics Educafion* Vol, 9(3), 1704-1709.
- [3] Mamidala, V., & Balachander, J. (2018). AI-driven software-defined cloud computing: A reinforcement learning approach for autonomous resource management and optimization. *International Journal of Engineering Research and Science & Technology*, 14(3).
- [4] Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2018). Detecting malicious domain names using deep learning approaches at scale. *Journal of Intelligent & Fuzzy Systems*, 34(3), 1355-1367.
- [5] Gaius Yallamelli, A. R., & Prasaath, V. R. (2018). AI-enhanced cloud computing for optimized healthcare information systems and resource management using reinforcement learning. *International Journal of Information Technology and Computer Engineering*, 6(3).
- [6] Yavuz, F. Y., Ünal, D., & Gül, E. (2018). Deep learning for detection of routing attacks in the internet of things. *International Journal of Computational Intelligence Systems*, 12(1), 39-58.
- [7] Gattupalli, K., & Lakshmana Kumar, R. (2018). Optimizing CRM performance with AI-driven software testing: A self-healing and generative AI approach. *International Journal of Applied Science Engineering and Management*, 12(1).
- [8] Gong, S., Cho, J., & Lee, C. (2018). A reliability comparison method for OSINT



- validity analysis. IEEE Transactions on Industrial Informatics, 14(12), 5428-5435.
- [9] Yalla, R. K. M. K., & Prema, R. (2018). ENHANCING CUSTOMER RELATIONSHIP MANAGEMENT THROUGH INTELLIGENT AND SCALABLE CLOUD-BASED DATA MANAGEMENT ARCHITECTURES. International Journal of HRM and Organizational Behavior, 6(2), 1-7.
- [10] Molanes, R. F., Amarasinghe, K., Rodriguez-Andina, J., & Manic, M. (2018). Deep learning and reconfigurable platforms in the internet of things: Challenges and opportunities in algorithms and hardware. IEEE industrial electronics magazine, 12(2), 36-49.
- [11] Sitaraman, S. R., & Pushpakumar, R. (2018). Secure data collection and storage for IoT devices using elliptic curve cryptography and cloud integration. International Journal of Engineering Research and Science & Technology, 14(4).
- [12] Dutta, S. (2018). An overview on the evolution and adoption of deep learning applications used in the industry. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 8(4), e1257.
- [13] Ganesan, T., & Hemnath, R. (2018). Lightweight AI for smart home security: IoT sensor-based automated botnet detection. International Journal of Engineering Research and Science & Technology, 14(1).
- [14] Resende, P. A. A., & Drummond, A. C. (2018). A survey of random forest based methods for intrusion detection systems. ACM Computing Surveys (CSUR), 51(3), 1-36.
- [15] Devarajan, M. V. (2018). AI-Powered Personalized Recommendation Systems for E-Commerce Platforms. International Journal of Marketing Management, 6(1), 1-8.
- [16] Barati, M., Abdullah, A., Udzir, N., Behzadi, M., Mahmood, R., & Mustapha, N. (2014). Intrusion detection system in secure shell traffic in cloud environment. Journal of Computer Science, 10(10).
- [17] Deevi, D. P., & Jayanthi, S. (2018). Scalable Medical Image Analysis Using CNNs and DFS with Data Sharding for Efficient Processing. International Journal of Life Sciences Biotechnology and Pharma Sciences, 14(1), 16-22.
- [18] Thampi, S. M., El-Alfy, E. S. M., Mitra, S., & Trajkovic, L. (2018). Soft computing and intelligent systems: Techniques and applications. Journal of Intelligent & Fuzzy Systems, 34(3), 1237-1241.
- [19] Gudivaka, R. K., & Rathna, S. (2018). Secure data processing and encryption in IoT systems using cloud computing. International Journal of Engineering Research and Science & Technology, 14(1).
- [20] Vinayakumar, R., Soman, K. P., Poornachandran, P., & Sachin Kumar, S. (2018). Detecting Android malware using long short-term memory (LSTM). Journal of Intelligent & Fuzzy Systems, 34(3), 1277-1288.
- [21] Panga, N. K. R. (2018). ENHANCING CUSTOMER PERSONALIZATION IN HEALTH INSURANCE PLANS USING VAE-LSTM AND PREDICTIVE ANALYTICS. International Journal of HRM and Organizational Behavior, 6(4), 12-19.
- [22] Ye, Y., Li, T., Adjeroh, D., & Iyengar, S. S. (2017). A survey on malware detection using data mining techniques. ACM Computing Surveys (CSUR), 50(3), 1-40.
- [23] Peddi, S., & Aiswarya, R. S. (2018). Securing healthcare in cloud-based storage for protecting sensitive patient data. International Journal of Information Technology and Computer Engineering, 6(1).
- [24] Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International



- Journal of Distributed Sensor Networks, 13(12), 1550147717741463.
- [25] Kodadi, S., & Kumar, V. (2018). Lightweight deep learning for efficient bug prediction in software development and cloud-based code analysis. *International Journal of Information Technology and Computer Engineering*, 6(1).
- [26] Rudd, E. M., Rozsa, A., Günther, M., & Boulton, T. E. (2016). A survey of stealth malware attacks, mitigation measures, and steps toward autonomous open world solutions. *IEEE Communications Surveys & Tutorials*, 19(2), 1145-1172.
- [27] Narla, S., & Kumar, R. L. (2018). Privacy-Preserving Personalized Healthcare Data in Cloud Environments via Secure Multi-Party Computation and Gradient Descent Optimization. *Chinese Traditional Medicine Journal*, 1(2), 13-19.
- [28] Pramanik, M. I., Lau, R. Y., Yue, W. T., Ye, Y., & Li, C. (2017). Big data analytics for security and criminal investigations. *Wiley interdisciplinary reviews: data mining and knowledge discovery*, 7(4), e1208.
- [29] Alavilli, S. K., & Pushpakumar, R. (2018). Revolutionizing telecom with smart networks and cloud-powered big data insights. *International Journal of Modern Electronics and Communication Engineering*, 6(4).
- [30] Al-rimy, B. A. S., Maarof, M. A., Prasetyo, Y. A., Shaikh, S. Z. M., & Ariffin, A. F. M. (2018). Zero-day aware decision fusion-based model for crypto-ransomware early detection. *International Journal of Integrated Engineering*, 10(6).
- [31] Nagarajan, H., & Kurunthachalam, A. (2018). Optimizing database management for big data in cloud environments. *International Journal of Modern Electronics and Communication Engineering*, 6(1).
- [32] Yang, L., Zheng, R., Zhu, J., Zhang, M., & Wu, Q. (2018). A Green Cloud Service Provisioning Method for Mobile Micro-Learning. *International Journal of New Technology and Research*, 4(4), 263080.
- [33] Srinivasan, K., & Arulkumaran, G. (2018). LSTM-based threat detection in healthcare: A cloud-native security framework using Azure services. *International Journal of Modern Electronics and Communication Engineering*, 6(2).
- [34] Patil, D. R., & Patil, J. B. (2015). Survey on malicious web pages detection techniques. *International Journal of u-and e-Service, Science and Technology*, 8(5), 195-206.
- [35] Musam, V. S., & Kumar, V. (2018). Cloud-enabled federated learning with graph neural networks for privacy-preserving financial fraud detection. *Journal of Science and Technology*, 3(1).
- [36] Xu, M., Song, C., Ji, Y., Shih, M. W., Lu, K., Zheng, C., ... & Kim, T. (2016). Toward engineering a secure android ecosystem: A survey of existing techniques. *ACM Computing Surveys (CSUR)*, 49(2), 1-47.
- [37] Alagarsundaram, P., & Arulkumaran, G. (2018). Enhancing Healthcare Cloud Security with a Comprehensive Analysis for Authentication. *Indo-American Journal of Life Sciences and Biotechnology*, 15(1), 17-23.
- [38] Song, C., Pons, A., & Yen, K. (2018). AA-HMM: An anti-adversarial hidden Markov model for network-based intrusion detection. *Applied Sciences*, 8(12), 2421.
- [39] Mandala, R. R., & N, P. (2018). Optimizing secure cloud-enabled telemedicine system using LSTM with stochastic gradient descent. *Journal of Science and Technology*, 3(2).



- [40] Zhauniarovich, Y., Khalil, I., Yu, T., & Dacier, M. (2018). A survey on malicious domains detection through DNS data analysis. *ACM Computing Surveys (CSUR)*, 51(4), 1-36.
- [41] Kethu, S. S., & Thanjaivadivel, M. (2018). SECURE CLOUD-BASED CRM DATA MANAGEMENT USING AES ENCRYPTION/DECRYPTION. *International Journal of HRM and Organizational Behavior*, 6(3), 1-7.
- [42] Jusas, V., Birvinskas, D., & Gahramanov, E. (2017). Methods and tools of digital triage in forensic context: Survey and future directions. *Symmetry*, 9(4), 49.
- [43] Budda, R., & Pushpakumar, R. (2018). Cloud Computing in Healthcare for Enhancing Patient Care and Efficiency. *Chinese Traditional Medicine Journal*, 1(3), 10-15.
- [44] Basatneh, R., Najafi, B., & Armstrong, D. G. (2018). Health sensors, smart home devices, and the internet of medical things: an opportunity for dramatic improvement in care for the lower extremity complications of diabetes. *Journal of diabetes science and technology*, 12(3), 577-586.
- [45] Subramanyam, B., & Mekala, R. (2018). Leveraging cloud-based machine learning techniques for fraud detection in e-commerce financial transactions. *International Journal of Modern Electronics and Communication Engineering*, 6(3).
- [46] Sadeghi, A., Bagheri, H., Garcia, J., & Malek, S. (2016). A taxonomy and qualitative comparison of program analysis techniques for security assessment of android software. *IEEE Transactions on Software Engineering*, 43(6), 492-530.
- [47] Radhakrishnan, P., & Mekala, R. (2018). AI-Powered Cloud Commerce: Enhancing Personalization and Dynamic Pricing Strategies. *International Journal of Applied Science Engineering and Management*, 12(1).
- [48] Xue, B., Zhang, M., Browne, W. N., & Yao, X. (2015). A survey on evolutionary computation approaches to feature selection. *IEEE Transactions on evolutionary computation*, 20(4), 606-626.
- [49] Dyavani, N. R., & Rathna, S. (2018). Real-Time Path Optimization for Autonomous Farming Using ANFTAPP and IoV-Driven Hex Grid Mapping. *International Journal of Advances in Agricultural Science and Technology*, 5(3), 86-94.
- [50] Jiang, S. (2018). On securing underwater acoustic networks: A survey. *IEEE Communications Surveys & Tutorials*, 21(1), 729-752.