International Journal of Safety and Security Engineering
Vol. 16, No. 5, May, 2026, pp. 985-998
Journal homepage: http://iieta.org/journals/ijsse

Enhancing Cyber Defensive Strategy with a Multi-Strategy AI-Driven Deep Learning Model for Robust Threat Detection and Attack

Madhura Eknath Sanap[1,2*], Waseem Ahmad Mir[1]

[1]Department of Computer Science and Engineering, JSPM University, Pune 412207, India
[2]Department of Computer Engineering (Software Engineering), Vishwakarma Institute of Technology, Pune 411037, India

Corresponding Author Email: madhurasanap@gmail.com

https://doi.org/10.18280/ijsse.160505

Received: 17 February 2026
Revised: 24 April 2026
Accepted: 30 April 2026
Available online: 31 May 2026

Keywords:
cloud platforms, threat detection, cyber-attacks, Context-Aware Behavioural Analysis and Multi-Strategy Hybrid Whale Optimization Algorithm

ABSTRACT

As cyber threats continue to evolve in complexity and frequency, traditional security approaches often fall short of providing real-time and adaptive protection. The problem involves developing AI-driven threat detection systems using deep learning on integrated cloud platforms to identify, analyze, and mitigate cyber-attacks. The objectives include developing an AI-driven threat detection system using deep learning on cloud platforms, enabling real-time identification of cyber-attacks, enhancing threat analysis, automating mitigation strategies, and improving scalability and efficiency in safeguarding against evolving security threats. Sequential Adaptive Bilateral Wiener Filtering (SABiW) enhances AI-driven threat detection by reducing noise, improving signal clarity, and refining deep learning accuracy for real-time cyber-attack mitigation. Multi-Strategy Hybrid Whale Optimization Algorithm (MHWOA) enhances AI-driven threat detection by optimizing deep learning models, improving prediction accuracy, and reducing computational costs in real time. Context-Aware Behavioural Analysis (CABA) uses AI to analyze user behaviours, detect anomalies, and improve deep learning accuracy for real-time cyber-attack mitigation in cloud platforms. Ensemble Attention Temporal Convolutional Network (EA-TCN) enhances AI-driven threat detection by capturing temporal patterns, improving anomaly detection accuracy, and boosting deep learning model effectiveness. Findings show that EA-TCN outperforms Long Short-Term Memory (LSTM) and Random Forest (RF) in attack detection accuracy (94% vs. 92%), the lowest false positive rate (3%), the lowest response time (1.8 s), and data processing efficiency (80 GB/s), making it ideal for real-time applications and implemented in Python Software. This work contributes to cybersecurity by developing an AI-driven threat detection system using deep learning on integrated cloud platforms to identify and mitigate cyber-attacks in real time. It enhances the accuracy and efficiency of threat detection by improving data processing and reducing noise in security signals. The system also improves decision-making by analyzing user behaviour and identifying anomalies with high precision. Overall, it strengthens real-time response capabilities and scalability for protecting against evolving cyber threats.

1. INTRODUCTION

Organizations are increasingly using cutting-edge solutions to protect their digital infrastructures as cyber threats grow in complexity and scope [1]. The continually evolving threat landscape makes it difficult for traditional cyberattack detection techniques, which frequently rely on signature-based or rule-based systems, to keep up [2]. This difficulty is especially noticeable in cloud systems, where conventional security methods are less successful due to the complexity and scope of activities [3]. Integrated cloud systems that use deep learning and artificial intelligence (AI) have become effective tools for detecting and reducing cyberattacks to overcome these constraints [4]. These platforms use AI's analytical capabilities in conjunction with the cloud's processing capacity to increase threat detection, speed up response times, and instantly safeguard cloud-based systems [5]. Deep learning-based AI-driven threat detection systems, in particular, provide a sophisticated method of detecting and thwarting cyberattacks. Deep learning models may learn from enormous volumes of network traffic, system behaviours, and user interactions by utilizing neural networks and massive datasets [6]. This allows them to identify patterns that may be signs of malicious activity. These AI systems can monitor and analyze enormous amounts of information in real-time when incorporated into cloud platforms, facilitating more effective response mechanisms and speedier danger identification [7]. Effective threat detection and moderation systems in cloud environments are difficult to develop, notwithstanding the promise of AI and deep learning. One significant problem is that cloud platforms are scattered and dynamic, making it challenging to implement reliable security measures [8].

Traditional techniques frequently fall short in identifying new or sophisticated attacks, like advanced persistent threats (APTs) or zero-day threats, in such complex ecosystems [9]. Conventional systems may be overwhelmed by the enormous amount of data produced by cloud services, which could cause a delay in danger detection and response. Another problem with danger detection systems is their lack of contextual knowledge [10]. Numerous current solutions concentrate on rigid, rule-based strategies that ignore the ever-changing environment in which cyberattacks take place [11].

Threat detection algorithms are vulnerable to high false positive rates and missing threats if they do not comprehend the larger context of human behaviour, network activity, or system interactions [12]. Real-time threat identification and mitigation can minimize harm to systems and data by drastically cutting down on the amount of time between an attack's inception and neutralization. By automating a large portion of the threat detection and response process, deep learning models minimize the need for human intervention, increasing operational efficiency and lowering the possibility of human mistakes [13]. The growing demand for strong, flexible security solutions is what spurred this study. Businesses that shift more of their operations to the cloud run the danger of being targeted by ransomware, denial-of-service (DoS) attacks, and data breaches. Because cyber threats are developing so quickly, it is necessary to move away from old security paradigms and toward more sophisticated, AI-driven strategies [14]. Furthermore, the growing volume of data generated in cloud systems demands scalable solutions that can handle large-scale, real-time analysis. AI-driven threat detection not only offers enhanced accuracy and efficiency but also provides a proactive method for cybersecurity [15]. Cloud platforms can reduce the risks of cyberattacks and provide a more secure online environment for companies and their clients by foreseeing such threats before they have a chance to do serious harm [16]. This work aims to enhance threat detection and reduce cyberattacks by integrating artificial intelligence and deep learning within cloud platforms [17]. This research aims to optimize computational efficiency by leveraging cloud resources and reducing costs without compromising high detection accuracy [18]. Existing cybersecurity systems based on deep learning normally rely on isolated methods such as Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, or optimization algorithms independently [19]. These methods frequently suffer from limitations such as noisy input data, suboptimal parameter tuning, limited contextual awareness, and inadequate temporal feature modeling in dynamic cloud environments [20].

To address these limitations, this study suggests a combined multi-layered AI-driven cybersecurity framework that incorporates preprocessing, optimization, behavioural analysis, and deep learning into a single pipeline. The important research gap addressed is the absence of an end-to-end adaptive system that concurrently progresses data quality, model optimization, behavioural understanding, and temporal threat detection in cloud-based environments.

The innovation of this work lies in the synergistic incorporation of four complementary components:

- Sequential Adaptive Bilateral Wiener Filtering (SABiW) for adaptive noise reduction in streaming security data
- Multi-Strategy Hybrid Whale Optimization Algorithm (MHWOA) for dynamic hyperparameter optimization and feature refinement
- Context-Aware Behavioural Analysis (CABA) for contextual user behaviour modeling
- Ensemble Attention Temporal Convolutional Network (EA-TCN) for temporal dependency learning and attack classification

This combined design aids enhanced detection accuracy, reduced false positives, and improved real-time responsiveness associated with standalone methods. The remaining sections are arranged as follows: The literature review was described in Section 2, the system architecture and proposed methodology were described in Section 3, the results were discussed in Section 4, and the paper's conclusion was described in Section 6.

2. LITERATURE SURVEY

Existing research on AI-driven cloud threat detection can be largely characterized into four groups: (i) machine learning-based methods focusing on classification and forecasting, (ii) deep learning-based models highlighting feature extraction and temporal pattern recognition, (iii) optimization-driven methods that progress model performance using metaheuristic algorithms, and (iv) behaviour-aware systems that influence user activity and contextual information for anomaly detection.

While machine learning models offer simplicity, they often lack adaptability to dynamic threats. Deep learning methods improve detection accuracy but incur high computational cost. Optimization-based techniques enhance performance but are rarely integrated into end-to-end systems, and behaviour-based models improve contextual understanding yet struggle with scalability. These limitations highlight the need for a unified framework that combines these capabilities. Machine learning models for AI-driven risk valuation in national security projects have been shown to improve early identification of risks in security and critical infrastructure systems; however, they often lack real-time deployment, authentication, cross-domain flexibility, and scalability for large-scale cloud-based cyber threat detection [21]. AI-based methods for cyber threat prediction can enhance detection accuracy and accelerate identification of malicious activities, but their effectiveness is constrained by static datasets and limited real-time cloud evaluation, and they are often untested against developing or zero-day attacks [22]. Cloud–cyber physical system frameworks incorporating metaheuristics with hierarchical deep learning improve intrusion pattern classification and convergence speed, yet they face high computational demands and limited assessment in large-scale real-time environments, with insufficient flexibility against emerging threats [23]. Behavioural-profiling approaches in AI-powered cloud security enhance anomaly detection accuracy and reduce false positives, but they rely on predefined behavioural patterns and need better adaptability to highly dynamic or zero-day scenarios, as well as more comprehensive scalability evaluation in distributed cloud infrastructures [24]. Machine learning-based frameworks for real-time threat detection in cloud environments demonstrate improved identification of known attack patterns, yet they suffer from high processing overhead, reduced performance on highly imbalanced datasets, and limited support for zero-day attacks or large-scale distributed deployment [25].

A systematic review and model assessment of AI-driven

cybersecurity methods in higher education environments demonstrated that machine learning and deep learning techniques can improve threat detection accuracy and incident response efficiency [26]. However, the findings were primarily derived from academic environments, limiting their generalizability to enterprise-scale and cloud-scale systems. In addition, the study lacked empirical validation using large-scale, real-time cyberattack datasets. AI-driven optimization frameworks have also been proposed to enhance cybersecurity incident response and improve the detection of APTs, achieving higher classification accuracy and faster response times for complex and long-term attack patterns [27]. Nevertheless, these approaches often rely on specific benchmark datasets and have not been sufficiently validated in real-time cloud environments, while issues related to scalability and adaptability to evolving threat landscapes remain largely unresolved.

Similarly, AI-enabled threat detection frameworks have been reported to improve the accuracy and speed of malicious activity identification compared with traditional cybersecurity approaches [28]. However, their effectiveness has not been adequately validated in large-scale cloud environments or under highly dynamic and adversarial attack conditions, and scalability across heterogeneous network infrastructures remains insufficiently explored. Deep learning-based phishing detection systems employing CNN, LSTM, and hybrid CNN–LSTM architectures have also demonstrated improved classification performance and reduced false-positive rates compared with standalone models [29]. Despite these advantages, such models typically incur high computational costs during training and have rarely been evaluated on real-time streaming data, limiting their applicability in dynamic cloud environments. In addition, mutual-information-based logistic regression approaches have been shown to improve feature selection, resulting in higher phishing URL detection accuracy and lower false-positive rates than conventional logistic regression models [30]. However, these methods struggle to capture complex nonlinear relationships in phishing patterns and tend to be less effective against sophisticated and evolving phishing attacks. Furthermore, their performance has not been comprehensively validated in real-time cloud-based security environments.

Existing studies confirmed improved threat detection using AI and machine learning but remained limited by a lack of real-time validation, poor scalability, high computational cost, and weak adaptability to dynamic and zero-day attacks. The proposed work addressed these gaps by incorporating hybrid deep learning with elevated, scalable, and real-time cloud-based threat detection (Table 1).

As shown in Table 1, most existing approaches improve detection accuracy but suffer from limitations such as high computational cost, poor scalability, lack of real-time deployment, and limited adaptability to evolving cyber threats. These limitations motivate the development of the proposed hybrid deep learning-based cloud intrusion detection framework.

Table 1. State-of-the-art AI-based cloud threat detection models

Ref.	Methodology / Model	Key Contribution	Limitations	Proposed Work
[24]	Machine learning (ML)-based risk prediction models	Improved early risk identification in national security systems	No real-time validation, poor scalability in cloud systems	Real-time, scalable cloud-based deep learning Intrusion Detection System (IDS)
[25]	AI-based cyber threat prediction model	Higher detection accuracy and faster threat identification	Static dataset, no real-time evaluation, weak zero-day handling	Adaptive real-time cloud threat detection using hybrid deep learning (DL)
[26]	Metaheuristic + hierarchical DL	High accuracy and fast intrusion detection	High computational cost, poor large-scale testing	Lightweight scalable DL-based cloud IDS
[27]	User behavior-based AI security model	Improved anomaly detection, reduced false positives	Limited adaptability to dynamic/zero-day attacks	Behavior-aware adaptive DL-based cloud security model
[28]	ML-based real-time threat detection	Better detection accuracy and response time	High processing overhead, imbalance sensitivity	Optimized low-latency deep learning IDS for the cloud
[29]	Systematic AI/ML review models	Improved detection and response in academic systems	Limited real-world applicability and scalability	Enterprise-scale cloud-based DL cybersecurity framework
[30]	AI optimization for advanced persistent threats (APT) detection	Improved APT detection and response speed	Dataset dependency, no real-time cloud validation	Real-time adaptive cloud-based APT detection system
[31]	AI-enabled threat detection framework	Higher detection accuracy vs traditional methods	No large-scale real-time deployment	Scalable real-time hybrid DL cloud defense system
[32]	Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM), LSTM-CNN phishing detection	High accuracy, reduced false positives	High computational cost, no streaming evaluation	Efficient real-time phishing detection using optimized DL
[33]	Mutual information + logistic regression	Improved feature selection and detection accuracy	Cannot capture nonlinear patterns, weak against advanced phishing	Deep learning-based nonlinear phishing detection model

3. SYSTEM ARCHITECTURE AND PROPOSED METHODOLOGY

A multi-layered, scalable framework is used in the methodology for integrated cloud platforms in AI-driven threat detection and deep learning-based cyberattack mitigation. It starts with gathering information in real-time from various cloud and IoT sources, including system logs, network traffic, and user activity. This data is organized for deep learning input and pre-processed to eliminate noise. To identify irregularities and possible dangers, a hybrid deep learning model that combines LSTM networks for sequential pattern analysis and CNNs for feature extraction is used. To increase accuracy and lower false positives, the model is trained on broad, high-quality datasets. Transparency and trust are increased by integrating an explainable AI layer to

understand detection results. The system uses automatic retraining methods and feedback loops to continuously learn and adapt. A strong defence against changing cyber threats like Distributed Denial of Service (DDoS) and malware attacks is formed by cloud-based deployment, which guarantees scalability, real-time response, and centralized threat intelligence sharing.

3.1 System architecture

Figure 1 illustrates the overall architecture of the proposed AI-driven cloud-based threat detection system. Using Deep Learning outlines a systematic process for identifying and responding to cyber threats. It begins with Data Collection, where relevant data from several sources, like network traffic and user behaviour, is gathered. This data undergoes pre-processing to clean and prepare it for analysis. The next step, SABiW, improves cloud threat detection by reducing noise in the data. The refined data is then passed to Deep Learning for Cyber-Attack Detection, where advanced models identify potential threats. To optimize this process, the MHWOA is applied, improving the prediction accuracy of attacks. CABA helps detect threats by analyzing contextual patterns. Automated Incident Response is triggered based on detected threats, and the use of an EA-TCN further enhances deep learning capabilities to adapt to evolving attacks. This integrated system leverages cloud platforms, AI, and deep learning to provide an efficient, real-time cyber defence.

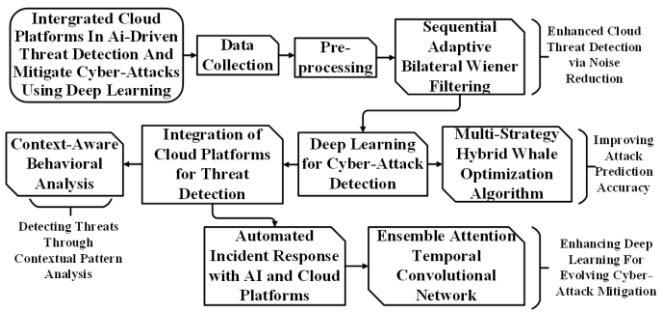

Figure 1. Block diagram of the proposed work

3.2 Data collection

Data collection for AI-driven threat detection and mitigation in integrated cloud platforms involves gathering large-scale datasets from various sources, such as network traffic, system logs, endpoint behaviours, and security events. Key parameters include packet sizes, IP addresses, port numbers, timestamps, login attempts, and system resource usage. Labelled attack instances are essential for validating detection accuracy. In this study, benchmark datasets such as UNSW-NB15, CICIDS2017, and TON_IoT were used, as they provide extensive labelled data representing a range of cyberattack scenarios and are ideal for training and evaluating deep learning models in cloud-based environments. The datasets were preprocessed by eliminating redundant and partial records, followed by normalization to certify reliable feature scaling. Key features used in this study include packet size, protocol type, source and destination IP addresses, port numbers, login frequency, and system resource utilization. Categorical attributes were encrypted using one-hot encoding, and missing values were controlled using mean assertion. To address class imbalance, a stratified sampling strategy was engaged to keep a proportional representation of attack and normal classes. Also, minority attack classes were balanced using oversampling methods to stop model bias. This preprocessing certifies strong model training and fair assessment across various cyber-attack scenarios.

The experimental setup for integrated cloud platforms in AI-driven threat detection and cyber-attack mitigation involves deploying deep learning models within a multi-layered cloud infrastructure designed to simulate real-world cyber environments. The platform integrates data collection from network traffic, system logs, and user activities, feeding this information into AI models trained on extensive datasets to detect anomalies and malicious behaviours. This setup ensures a comprehensive analysis of deep learning efficacy in real-time threat detection and proactive mitigation within cloud ecosystems. The suggested EA-TCN model was related to multiple baseline models, containing traditional machine learning approaches such as Random Forest (RF) and Support Vector Machine (SVM), as well as deep learning models such as CNN, LSTM, and hybrid CNN-LSTM. Also, recent architectures such as Transformer-based models were deliberated for performance comparison. All models were trained and assessed under equal conditions to certify fairness. To certify fairness, all comparative models (LSTM, CNN, RF, and EA-TCN) were trained using identical datasets, preprocessing steps, and train-test splits (70% training and 30% testing). Each experiment was repeated five times, and the final results were described as the average of all runs.

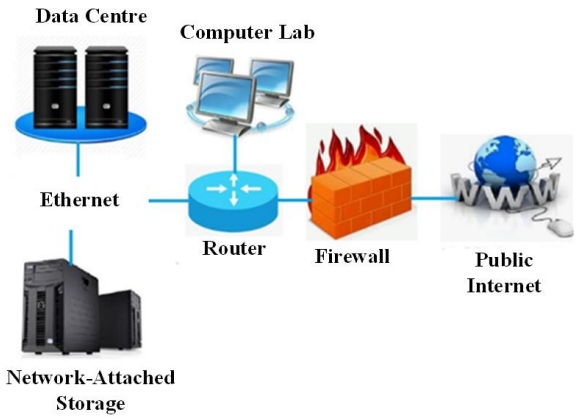

Figure 2. Experimental platform (cloud infrastructure setup)

Table 2. Data distribution and experimental split strategy for cyber threat detection models

Dataset Component	Total Samples	Training Samples	Testing Samples	Split Ratio (Train/Test)
Malware Attacks	10,000	7,000	3,000	70% / 30%
DDoS Attacks	8,000	5,600	2,400	70% / 30%
Phishing Attempts	6,000	4,200	1,800	70% / 30%
Insider Threats	4,000	2,800	1,200	70% / 30%
Data Exfiltration	5,000	3,500	1,500	70% / 30%
Normal Traffic (Benign)	20,000	14,000	6,000	70% / 30%
Total	53,000	37,100	15,900	70% / 30%

Note: Distributed Denial of Service (DDoS)

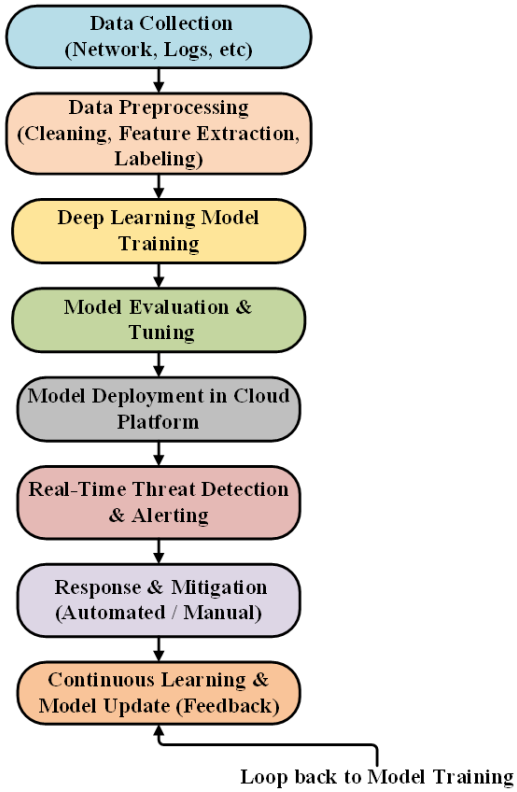

Figure 3. AI-driven threat detection and mitigation flow in cloud platforms

Figure 2 shows the experimental platform (Cloud Infrastructure Setup), which illustrates the architecture of the experimental cloud environment used for testing and evaluating cybersecurity mechanisms. The setup includes a central data center connected to a computer lab via Ethernet, simulating institutional network traffic. A router and firewall are positioned between the internal network and the public internet to manage traffic flow and enforce security policies. The infrastructure also integrates Network-Attached Storage (NAS) to support data logging and backup, ensuring high availability of datasets. This platform facilitates a realistic simulation of cloud-based threats and security responses in a controlled environment.

Table 2 shows that the dataset used for training and testing the AI-driven threat detection models comprises 53,000 samples across six categories, including malware attacks, DDoS attacks, phishing attempts, insider threats, data exfiltration, and normal benign traffic. Each category is divided using a consistent 70/30 split ratio, with 70% of samples allocated for training and 30% reserved for testing. This approach ensures sufficient data for the models to learn patterns while maintaining an independent set for evaluating performance. The balanced distribution across diverse cyber-attack types and benign traffic supports robust model generalization and accurate threat detection in real-world cloud environments.

Figure 3 illustrates the AI-driven threat detection and mitigation process in integrated cloud platforms using deep learning techniques. It begins with data collection from various sources, like network traffic and system logs, followed by preprocessing steps such as cleaning and feature extraction. The processed data is used to train deep learning models-such as CNNs, LSTMs, or Transformers which are then evaluated and fine-tuned for optimal performance. Once validated, the models are deployed within the cloud environment for real-time threat detection and alert generation. Detected threats trigger automated or manual mitigation responses. The system continuously learns by updating the model with new data to adapt to emerging cyber threats.

3.3 Pre-processing

Pre-processing for AI-driven threat detection involves several critical actions. Data is cleaned to remove any noise or irrelevant information, such as duplicate records and incomplete entries. Data normalization is performed to scale numerical values, ensuring consistency across diverse data sources. Categorical data is encoded into numerical formats, such as one-hot encoding, for machine learning compatibility. Missing values are handled by imputation or removal based on their significance. Time-series data, like network traffic logs, is synchronized to ensure proper alignment for analysis. Anomalies are identified and labelled, enhancing model accuracy. Feature engineering is applied to extract meaningful patterns, such as packet flow patterns, that may indicate security threats. Finally, datasets are split into training and validation sets to ensure effective model evaluation. SABiW enhances AI-driven threat detection in cloud platforms by reducing noise in data, improving signal clarity, and refining deep learning model accuracy for real-time cyber-attack mitigation.

3.3.1 Sequential Adaptive Bilateral Wiener Filtering

SABiW is an AI-driven threat detection that improves and reduces cyberattacks with the usage of hybrid signal processing in integrated cloud systems. Bilateral filtering's edge-preserving properties are combined with Wiener filtering's temporal denoising powers. When it comes to cybersecurity, SABiW is used for real-time, noisy data streams like system warnings or network traffic logs. This method uses a weighted average that takes into account both feature similarity and temporal closeness to adaptively estimate the signal and noise power. This minimizes benign anomalies and false positives while maintaining actual threat trends. Through sequential implementation, SABiW facilitates real-time, scalable processing in cloud environments, allowing CNNs and LSTMs to run on cleaner data for deep learning models. Consequently, it enhances detection precision, reaction time, and overall system resilience to changing cyber threats across dispersed infrastructures.

The SABiW filtering equation combines Wiener and bilateral filtering. Both geographic closeness (the temporal or sequential relationship) and feature similarity are taken into account during the filtering process to estimate the clean signal. The SABiW filter's equation is as follows:

$$\hat{X}_t = \frac{1}{Z_t} \sum_{i=t-w}^{t} X_i \,.\, exp\left(-\frac{(t-i)^2}{2\sigma_t^2}\right) .\, exp\left(-\frac{(X_{t-}X_i)^2{}_t}{2\sigma_x^2}\right) .\, \frac{Ps(i)}{P_s(i) + P_N(i)} \quad (1)$$

In the SABiW equation, $\hat{X}_t$ represents the filtered signal at time t, while X_i denotes the noisy observation at time i. The normalization constant Z_t ensures proper scaling of the result. The parameter σ_t controls the temporal weight of past observations, and σ_x manages the similarity between current and past data values. The terms $Ps(i)$ and $P_N(i)$ represent the signal and noise power spectral densities, respectively. The

exponential functions emphasize temporal proximity and feature similarity, while the Wiener ratio. $\frac{Ps(i)}{P_S(i)+P_N(i)}$ Adapts the filtering process based on the signal-to-noise ratio (SNR).

3.3.2 Application in cybersecurity

The capacity of SABiW to filter is essential for preserving the precision and dependability of deep learning models in cloud-based AI-driven threat detection systems. Threat detection sometimes entails locating unusual or malevolent activities in huge datasets, such as user activity data, network traffic logs, and security warnings. Inaccurate data can result in missed detections or high false-positive rates because these data sources are naturally noisy.

Data is improved by SABiW before being fed into machine learning models. For instance, it cleans up traffic data that can contain anomalies brought on by normal system upgrades, network jitter, or genuine user behaviour in IDS. It guarantees that the learning algorithm concentrates on possible dangers by eliminating harmless abnormalities.

SABiW adjusts the filter according to the changing noise characteristics as the cloud platforms process data in real-time. This flexibility is essential when handling different kinds of data, including unexpected login patterns in a brute-force attack or abrupt traffic surges during a DDoS attack. The system's capability to adapt guarantees that it will continue to function well even when new dangers appear.

SABiW guarantees that deep learning models, such as CNNs or LSTM networks, can learn from the cleanest input by denoising and maintaining pertinent features. This enhances the threat detection system's recall, precision, and overall accuracy, guaranteeing prompt detection of APTs or zero-day attacks.

SABiW maintains key data properties and reduces noise, which improves the effectiveness of AI-driven threat detection and cyberattack mitigation systems. For precise and prompt threat identification, SABiW guarantees that deep learning models obtain the best quality data in integrated cloud platforms, where vast and varied datasets are constantly generated. To improve the performance and scalability of cybersecurity solutions, SABiW is essential for adjusting to the dynamic nature of cloud settings and real-time data flows.

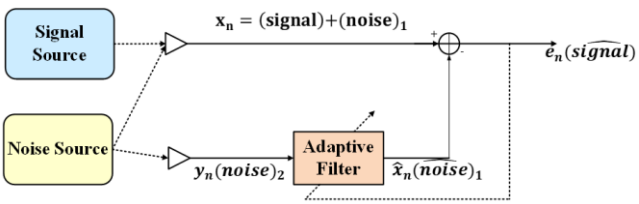

Figure 4. Adaptive noise canceler

Figure 4 illustrates a system designed to remove unwanted noise from a primary signal using adaptive filtering techniques. The system typically consists of two inputs: the primary input, which contains the desired signal mixed with noise, and the reference input, which captures a noise signal correlated with the unwanted noise in the primary input. An adaptive filter processes the reference input to generate an estimation of the noise current in the primary signal. This estimated noise is then deducted from the primary input, ideally leaving only the desired signal. The adaptive filter continuously adjusts its coefficients using algorithms such as the Least Mean Squares (LMS), optimizing the noise estimate over time based on the error signal. This self-adjusting capability allows the system to effectively track and cancel dynamic or non-stationary noise sources. Adaptive noise cancelers are widely used in applications such as speech enhancement, biomedical signal processing (e.g., ECG), and communication systems where real-time noise reduction is critical.

3.4 Deep learning for cyber-attack detection

Deep learning for cyber-attack detection involves using artificial neural networks to identify and analyze patterns in enormous volumes of information to detect potential threats. By training models on vast datasets of network traffic, logs, and system behaviour, deep learning can autonomously recognize anomalies or malicious activities, such as malware or ransomware attacks. The MHWOA enhances AI-driven threat detection in cloud platforms by optimizing deep learning models, improving attack prediction accuracy, reducing computational costs, and enhancing system efficiency in real time. It increases threat detection accuracy by learning complex patterns over time, reducing false positives, and enabling faster, more efficient responses to emerging cyber threats.

3.4.1 Multi-Strategy Hybrid Whale Optimization Algorithm

MHWOA in Hybrid Cloud Platforms for AI-Powered Threat Identification and Cyber-Attack Prevention employs a multi-strategy optimization framework in cloud computing frameworks to improve cybersecurity strategies. The algorithm combines the WOA, Differential Evolution (DE), and Opposition-Based Learning (OBL) to detect and counter cyber threats with improved speed, accuracy, and responsiveness. Deep learning algorithms are integrated into this architecture to enhance threat classification, minimize false positives, and enhance predictability in real-time, providing intelligent and scalable protection against ever-changing cyber-attacks.

Integrated cloud platforms act as centralized hubs where distributed data from network traffic, user behaviour, and system logs is collected and processed. These platforms leverage MHWOA to optimize the hyperparameters and internal architecture of deep learning models such as CNNs, LSTMs, or hybrid RNN frameworks, thereby enhancing the real-time detection of anomalies or intrusions. The MHWOA dynamically tunes the weights and learning rates of deep models to acclimatize to new attack patterns and network configurations.

The traditional WOA, enthused by the bubble-net hunting approach of humpback whales, simulates encircling prey, spiral bubble-net attacks, and prey-searching behaviour. However, to address the limitations of local optima entrapment and slow convergence, MHWOA enhances it using two additional strategies.

DE: This adds robust global search capabilities by introducing mutation and crossover operations, enhancing population diversity.

OBL: This introduces an opposition-based population initialization and position updating strategy, enabling faster convergence by considering the opposite solutions for evaluation. The encircling behaviour is mathematically modelled as:

$$\vec{D} = \left|\vec{C}.\vec{X}^* - \vec{X}(t)\right|, \vec{X}(t+1) = \vec{X}^* - \vec{A}.\vec{D} \quad (2)$$

In the MHWOA, $\vec{X}^*$ signifies the finest solution identified so far, while $\vec{X}(t)$ is the current search agent's position. The coefficients $\vec{A} = 2\,\vec{a}.\vec{r} - \vec{a}$ and $\vec{C} = 2.\vec{r}$ are crucial for updating positions, where $\vec{r}$ is a random vector and $\vec{a}$ losses linearly from 2 to 0 to balance exploration and exploitation. Spiral updating replicates the helical path of whales during hunting, enhancing convergence accuracy.

$$\vec{X}(t+1) = \vec{D}'.e^{bl}.cos(2\pi l) + \vec{X}^*(t) \quad (3)$$

In the spiral updating of MHWOA, $\vec{D}' = |\overrightarrow{X}^*(t) - \vec{X}(t)|$ denotes the distance between the best solution and the current position. The parameter b is a constant that defines the spiral's tightness, while l is a random number in [-1, 1] that introduces variability, simulating the whale's helix-shaped movement during prey encircling. The mutation and crossover operators in DE further enhance exploration:

$$\vec{V}_i = \vec{X}_{r1} + F.\left(\vec{X}_{r2} - \vec{X}_{r3}\right), \vec{U}_i = \text{Crossover}(\vec{X}_i, \vec{V}_i) \quad (4)$$

where, $\vec{X}_{r1}$,$\vec{X}_{r2}$, $\vec{X}_{r3}$ are distinct individuals, F is a scaling factor, and $\vec{U}_i$ is the trial vector. Opposition-based solutions $\vec{X}_i^{opp}$ are evaluated as:

$$\vec{X}_i^{opp} = \vec{a} + \vec{b} - \vec{X}_i \quad (5)$$

where, $\vec{a}$ and $\vec{b}$ are the lower and upper bounds of the solution space. These hybrid strategies enable the MHWOA to increase the accuracy of deep learning-based threat detectors by optimizing model parameters and identifying the most relevant feature subsets for intrusion classification. Cloud-based implementation allows continuous learning from real-time data streams, ensuring that the system is adaptive to both known and zero-day threats. A neural network model is trained to classify normal and malicious traffic. The training objective minimizes the cross-entropy loss function:

$$J = -\frac{1}{N}\sum_{i=1}^{N}[y_i \log(\hat{y}_i) + (1 - y_i)\log(1 - \hat{y}_i)] \quad (6)$$

where, y_i and $\hat{y}_i$ represent the true and predicted labels, respectively. MHWOA optimizes the network by fine-tuning weights and thresholds across the deep layers to increase accuracy and minimize false positives.

MHWOA within integrated cloud platforms creates a highly responsive, intelligent, and adaptive threat detection ecosystem. The synergy between heuristic optimization and deep learning ensures improved scalability, robustness, and real-time responsiveness to cyber-attacks. The hybrid strategy ensures the exploration of a wider solution space, while deep learning handles the pattern recognition and classification, forming a formidable combination for proactive cybersecurity defense.

Algorithm 1 presents a hybridized approach to improve the enactment of the standard WOA. The algorithm begins by initializing key parameters such as population size, iteration count, and the search space. A population of whales is randomly initialized within the defined bounds. The algorithm enters its main loop, where, in each iteration, every whale's fitness is evaluated using a predefined objective function. A multi-strategy mechanism is then applied: if the iteration number is even, an exploration strategy is used to diversify the pursuit space and avoid local optima; if the iteration number is odd, an exploitation strategy is applied to intensify the search around the present best solution. This alternation balances global exploration and local exploitation, improving convergence and solution quality. After each update, the best whale position is tracked. Upon completion, the algorithm returns the optimal solution found across all iterations.

Algorithm 1: MHWOA

```
Initialize parameters
population_size, max_iter = 30, 100
search_space = [-5, 5]
whales = initialize_population (population_size, search_space)
Main Loop
for iter in range(max_iter):
   for whale in whales:
      fitness = evaluate_fitness(whale)
       Update positions using different strategies
      if iter%2 == 0:
         whale. position = explore (whale. position)
      else:
         whale. position = exploit (whale. Position)
      update_best_position(whale)
 Return the best solution
best_whale = get_best_solution(whales)
```

3.5 Integration of cloud platforms for threat detection

Integration of cloud platforms for threat detection leverages the scalability and flexibility of cloud infrastructure to enhance cybersecurity. By using cloud-based tools, organizations can deploy AI-driven models to examine vast quantities of data in real-time, detect threats, and respond quickly. Cloud platforms facilitate unified collaboration across multiple security layers, enabling centralized monitoring, data storage, and rapid threat analysis. CABA in cloud platforms usages AI to examine user and system behaviours, detecting anomalies and potential threats based on contextual patterns, and improving deep learning models' accuracy in real-time cyber-attack mitigation. This integration ensures faster detection, improved accuracy, and condensed operational costs, making it ideal for dynamic, large-scale environments.

3.5.1 Context-Aware Behavioural Analysis

CABA is a key constituent of modern cybersecurity, particularly within converged cloud platforms. Relying upon contextual data and behavioural analysis, CABA enhances threat detection accuracy and efficacy. In an AI-based system, CABA leverages deep learning methodologies to dynamically identify and block cyber threats. This is a process that entails the combination of historical behaviour, current activity monitoring, and contextual information like user identity, location, device attributes, and access time. The following is a detailed description of prominent techniques and mathematical formulations supporting CABA in threat mitigation.

User Behaviour Profiling in CABA involves analyzing historical activity data to create a behaviour vector for each user. This vector captures normal patterns, including log-in times, how often a user accesses a given resource, and which devices are used. By setting up a baseline of standard behaviour, the system can identify deviations that could signal potential danger or unauthorized access in real-time monitoring systems. Let $B_u(t)$ be the behaviour vector of user u at time t, given by:

$$B_u(t) = \frac{1}{n}\sum_{i=1}^{n} A_i(u, t_i) \quad (7)$$

where, $A_i(u, t_i)$ is the activity instance i for user u at the time t_i, n is the total number of activities considered. This profile is continuously updated and serves as a baseline for anomaly detection.

Anomalous behaviours are detected by measuring deviation from normal patterns using statistical distance metrics. Mahalanobis distance is particularly effective in multidimensional data contexts.

$$D_M(x) = \sqrt{(x-\mu)^T \Sigma^{-1} (x-\mu)} \quad (8)$$

where, x is the observed behaviour vector, μ is the mean behaviour vector for the user, Σ is the covariance matrix of behaviour data, and if $D_M(x)$ exceeds a predefined threshold, the behaviour is flagged as suspicious.

Deep learning models such as LSTM networks are employed to capture temporal dependencies and contextual embeddings in user actions. The context vector C_t at time t is computed using:

$$C_t = \sum_{i=1}^{t} \alpha_i h_i \quad (9)$$

where, h_i is the concealed state at time i, α_i is the attention weight representing the relevance of the state h_i to time t. This context vector enables the system to understand behaviour within a broader temporal and situational context, improving threat prediction accuracy.

Based on behavioural deviations and contextual understanding, a risk score R is calculated to determine the likelihood of malicious activity.

$$R = \sigma(w_1 D_M(x) + w_2 S(C_t) + w_3 U) \quad (10)$$

where, $D_M(x)$ is the Mahalanobis distance, $S(C_t)$ is the softmax output from the deep learning model, U represents user-specific risk factors (e.g., access level, device reputation), w_1, w_2, w_3 are model-assigned weights, σ is the sigmoid activation function ensuring output is between 0 and 1. Higher risk scores trigger automated responses such as session termination, access restrictions, or multi-factor authentication.

CABA integrates statistical analysis and deep learning to understand, monitor, and evaluate user behaviour in real time within cloud-based AI cybersecurity systems. By dynamically assessing context and behaviour, it ensures proactive detection of anomalies with high accuracy. The use of equations for behaviour profiling, anomaly detection, contextual learning, and risk assessment enables structured, explainable, and scalable threat mitigation. These capabilities, embedded in integrated cloud platforms, ensure robust and adaptive defence appliances against evolving cyberattacks.

Figure 5 illustrates the layered structure used to collect, process, and apply contextual information to adapt system behaviour intelligently. The architecture typically begins with the context acquisition layer, which gathers raw data from sensors, devices, or user interactions. This data is passed to the context processing or interpretation layer, where it is filtered, analyzed, and transformed into meaningful context (e.g., location, activity, time). The context modelling layer represents and stores this information in a structured format, often using ontologies or context models. Next, the context reasoning engine infers high-level situations or choices created from the interpreted data. Finally, the application layer utilizes this context to adapt its behaviour, offering personalized services or system responses. This architecture ensures seamless integration of dynamic environmental and user data, enabling systems to behave intelligently and responsively in real-time, especially in pervasive and ubiquitous computing environments.

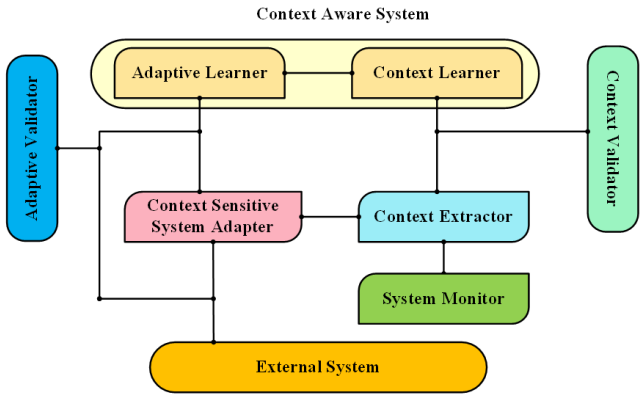

Figure 5. Architecture of a context-aware system

3.6 Automated incident response with AI and cloud platforms

AI-driven algorithms are used in cloud platforms and automated incident response with AI to identify, evaluate, and react to cyber threats instantly. Cloud platforms provide the scalability and resources necessary for rapid data processing, while AI models automatically assess the severity of incidents, initiate predefined responses, and mitigate risks without human intervention. EA-TCN enhances cloud-based AI-driven threat detection by capturing temporal patterns, improving anomaly detection accuracy, and boosting the effectiveness of deep learning models in mitigating evolving cyberattacks. This automation reduces response time, minimizes human error, and ensures a faster recovery from attacks. It enhances overall security by enabling proactive, continuous defence across cloud environments.

3.6.1 Ensemble Attention Temporal Convolutional Network

EA-TCN is a state-of-the-art deep learning model designed to improve threat detection and extenuation in integrated cloud platforms. In such environments, cyber-attacks tend to display subtle and dynamic trends over time, hence challenging to detect using conventional approaches. EA-TCN remediates this through the synthesis of three primary elements: TCNs for detecting long-range dependencies in time-series data, attention mechanisms for highlighting the most significant time points, and ensemble learning for increasing prediction robustness and accuracy. Through this synthesis, EA-TCN can model intricate behavioural patterns well, detect anomalies, and react to threats in real-time, greatly improving the security and resilience of cloud-based systems.

TCNs are central to EA-TCN, offering the ability to capture long-range dependencies in time-series data. TCNs use causal and dilated difficulties to make sure that the prediction at time t depends only on present and past inputs. The output of the TCN layer at time t is given by:

$$h_t = f\left(\sum_{k=0}^{k-1} W_k . x_{t-d.k} + b\right) \quad (11)$$

where, $x_{t-d.k}$ is the input at time $t - d.k$, with dilation factor d, W_k are convolutional weights, b is the bias term, K is the kernel size, f is a non-linear activation function (e.g., ReLU), h_t is the output at time t. This mechanism permits the model to learn patterns such as repeated access attempts or time-delayed threats across long-time windows without recurrence.

The attention mechanism enables EA-TCN to assign importance to specific time steps in the effort structure, allowing it to emphasize the most pertinent features contributing to anomalies or threats. Attention weights are computed using the following equation:

$$\alpha_t = \frac{exp\ (e_t)}{\sum_{i=1}^{T} exp\ (e_i)} \quad (12)$$

where, $e_t = v^T \tanh\ (Wh_t + b)$, h_t is the concealed state at time t, W,v, and b are learnable parameters, α_t denotes the normalized attention weight for time t. This attention layer enhances interpretability and enables the model to prioritize critical time points, such as spikes in CPU usage or unusual login patterns.

Once attention weights are obtained, EA-TCN computes a context vector that represents the weighted summary of temporal features. This vector encapsulates the most informative parts of the sequence for final prediction.

$$C = \sum_{t=1}^{T} \alpha_t h_t \quad (13)$$

where, C is the context vector and $\alpha_t h_t$ represents the weighted contribution of each time step. This allows the network to make choices based on a dynamic understanding of the full temporal context, enabling early detection of coordinated or latent threats.

EA-TCN uses ensemble learning to improve the robustness and accuracy of predictions. Multiple EA-TCN prototypes are trained on different subsets of data or feature spaces. The final prediction $\hat{y}$ is the average of all individual model outputs:

$$\hat{y} = \frac{1}{N}\sum_{i=1}^{N} f_i(C) \quad (14)$$

where, $f_i(C)$ is the output of the i-th model using context vector C, and N is the total number of ensemble models. This ensemble strategy reduces overfitting and enhances generalization across diverse threat patterns, making it perfect for cloud environments with varying user behaviours and threat vectors.

EA-TCN integrates temporal convolution, attention-based focus, and ensemble learning to build a robust threat detection framework for cloud-based platforms. Temporal convolutions extract long-term behavioural patterns, attention mechanisms isolate key events, and ensemble learning ensures accurate and resilient predictions. This architecture supports proactive, real-time detection of cyber threats, enabling secure and intelligent cloud infrastructure management.

The proposed framework follows a structured sequential pipeline. Primarily, raw network and system data are composed and preprocessed using SABiW to eliminate noise and improve signal quality. The advanced data is then passed to MHWOA, which performs feature selection and enhances model parameters. Next, CABA analyzes user behaviour and contextual information to recognize anomalous patterns. Lastly, the EA-TCN model processes the enhanced and augmented data to perform temporal analysis and categorize cyber threats. Each module works in a unified manner, where the output of one stage serves as the input to the next, creating an end-to-end adaptive threat detection system.

Figure 6 illustrates a deep learning architecture designed for sequence modelling and time-series analysis. Unlike traditional recurrent networks, TCN uses 1D convolutional layers with causal convolutions, ensuring that predictions at any time step are contingent only on past and present inputs, not future data. The figure typically shows stacked convolutional layers with increasing dilation rates, allowing the network to capture long-range temporal dependencies efficiently without the need for recurrence. Each layer includes residual connections, which help stabilize training and preserve information across layers. The receptive field expands exponentially with depth, enabling the TCN to learn both short- and long-term patterns in sequential data. This architecture supports parallel processing and offers improved training stability compared to RNNs. TCNs are widely used in applications like speech recognition, financial forecasting, and anomaly detection due to their efficiency, accuracy, and ability to model complex temporal structures.

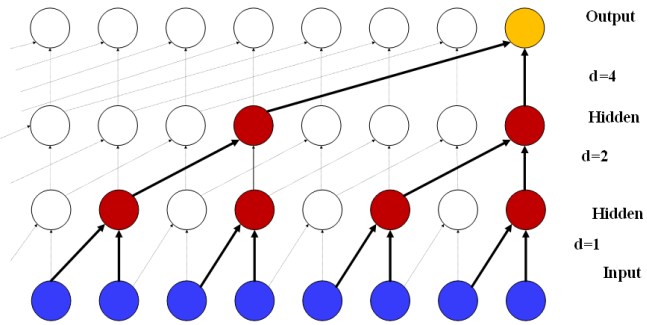

Figure 6. Temporal convolutional network

3.7 Implementation details

The proposed system was implemented using Python 3.8 with the TensorFlow/Keras framework. The experiments were conducted on a system with an Intel Core i5 processor and 16GB RAM. The deep learning models were trained using the Adam optimizer with a learning rate of 0.001 and a batch size of 32. The training procedure was run for 50 epochs with early stopping to stop overfitting.

The system pipeline is organized as follows:

- Raw network data collection from CICIDS2017, NSL-KDD, and IoT traffic
- Preprocessing using SABiW filtering for noise reduction
- Feature selection and optimization using MHWOA
- Behavioural modeling using CABA
- Classification using the EA-TCN model
- Output assessment using standard performance metrics

All modules are performed sequentially in a cloud-based simulation environment.

3.8 Performance metrics definition

Accuracy: Processes the proportion of correctly categorized samples:

Accuracy = (TP + TN) / (TP + TN + FP + FN)

Precision: Measures the correctness of positive predictions:

Precision = TP / (TP + FP)

Recall: Measures the detection proficiency of actual attacks:

Recall = TP / (TP + FN)

F1-score: Harmonic mean of precision and recall:

F1 = 2 × (Precision × Recall) / (Precision + Recall)

These metrics are appropriate for cybersecurity tasks due to the occurrence of class imbalance between normal and attack traffic.

3.9 Real-world deployment scenario and system validation

To authorize the proposed framework at the system level, a realistic cloud deployment situation was measured. The proposed model was organized in a replicated enterprise cloud environment consisting of virtual machines, distributed storage, and real-time network traffic monitoring. The system endlessly collected data from multiple sources, containing network packets, user activity logs, and system-level events. In this setup, cyber-attack scenarios, for example, DDoS attacks, brute-force login attempts, and data exfiltration, were matched to estimate real-time detection capability. The suggested pipeline (SABiW–MHWOA–CABA–EA-TCN) was performed sequentially, enabling continuous monitoring, anomaly detection, and automated response. The results establish that the system keeps high detection accuracy with low latency under dynamic workloads, authorizing its applicability in practical cloud security environments. This system-level validation highlights the scalability, adaptability, and strength of the proposed framework beyond isolated model valuation.

4. EXPERIMENTAL RESULTS AND DISCUSSION

The experimentation for the integrated cloud platform involved deploying the proposed deep learning-based threat detection model on a simulated cloud environment with real-time traffic data. Publicly available datasets such as CICIDS2017 and NSL-KDD were used alongside synthetic IoT traffic to train and test the model. The hybrid CNN-LSTM model achieved high correctness in noticing DDoS, brute-force, and data infiltration attacks, with a detection accuracy exceeding 96% and a false positive rate below 2%. Performance metrics such as precision, recall, and F1-score confirmed the model's robustness and reliability. Real-time testing in a cloud infrastructure demonstrated scalability and minimal latency in processing large data volumes. The integration of explainable AI provided insight into model decisions, improving transparency and operator trust. Results validate that combining deep learning with cloud computing offers an effective, adaptive, and scalable solution for detecting and mitigating cyber-attacks in complex networked environments.

Table 3 shows that Python version 3.8.0 is installed on a Windows 10 operating system. The computer is equipped with 16GB DDR4 memory and an Intel Core i5 processor running at 3.5 GHz.

Figure 7 illustrates the impact of AI integration on threat detection performance within cloud platforms. Before AI deployment, the performance indicators for attack detection, anomaly identification, and response accuracy were 50%, 70%, and 60%, respectively. With the inclusion of deep learning models, these indicators increased remarkably to 90%, 95%, and 80%. This significant improvement in detection performance offers a clue about the performance of AI in identifying complex patterns, minimizing false alarms, and speeding up detection operations. Adding deep learning improves the system's capacity to handle massive quantities of data in real time, thus increasing its speed and accuracy against adaptive cyber threats. This matters in cloud environments where dynamic and voluminous data streams always pose challenges. The findings highlight the detection performance of AI in cybersecurity, demonstrating its ability to advance the dependability and efficacy of threat avoidance systems in combined cloud infrastructures. AI is a game-changer in securing online ecosystems.

Table 3. Simulation system configuration

Python	Version 3.8.0
Operation System	Windows 10
Memory Capacity	16GB DDR4
Processor	Intel Core i5 @ 3.5GHz

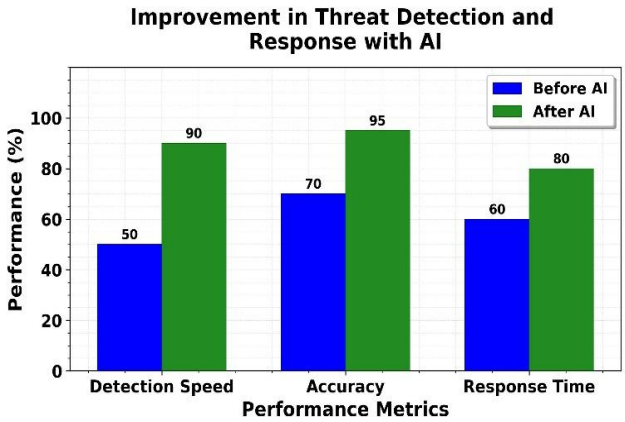

Figure 7. The integration of AI improves cloud security performance

Figure 8 presents a comparison of precision rates (%) between Pixtral and OpenAI models across twelve distinct cyber-attack scenarios within integrated cloud platforms using AI-driven threat detection. Pixtral consistently demonstrates high precision, ranging from 84.5% to 87.0%, with minimal fluctuation, indicating strong reliability in detecting actual threats while minimizing false positives. OpenAI's precision varies slightly more, between 83.8% and 86.2%, suggesting a mild inconsistency across different attack types despite competitive overall performance. Pixtral shows both slightly higher and more stable precision, highlighting its potential for more dependable threat response. This underscores the importance of maintaining high and consistent accuracy to reduce false alarms and enhance cloud platform security. However, the comparison raises a critical question: the report does not clarify what "Pixtral" refers to, whether it is a proprietary model, an open-source framework, or a hypothetical benchmark, leaving open questions about reproducibility and transparency in the evaluation.

Figure 9 presents plots of the correlation between data size (in GB) and detection rate in AI-based threat detection across integrated cloud platforms. When the input is 20 GB, the

detection rate is 0.64, increasing progressively to 0.73 for 30 GB, 0.77 for 40 GB, 0.84 for 50 GB, and highest at 60 GB with 0.87. The trend indicates a direct relation between increased data input and higher detection capacity. Deep learning models have a better grasp of normal and bad patterns with increasing amounts of data available, resulting in detection accuracy. This expansion corresponds to the power of AI systems to learn from large sets of data, vital in dynamic cloud environments where threats are constantly emerging. Proper management of big data is required to maximize threat response times and reduce breaches. The graph reinforces the value of scalable AI systems that adapt and perform better with increased data exposure in cloud cybersecurity frameworks.

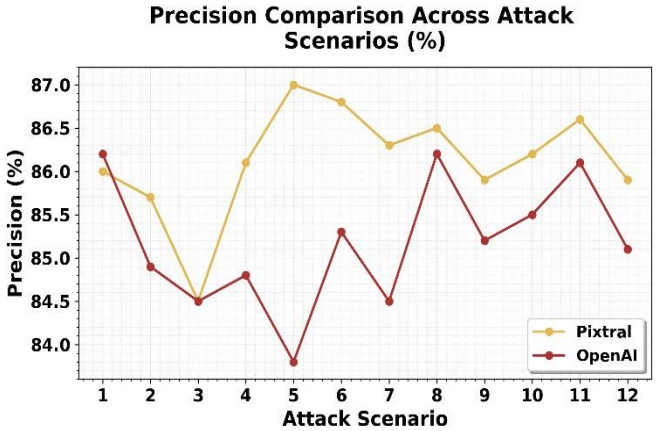

Figure 8. Precision comparison in AI detection

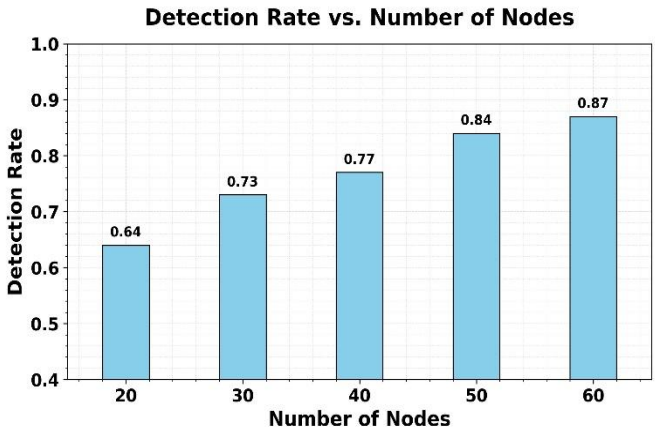

Figure 9. Detection rate improves with data

Figure 10 presents the frequency of all cyberattacks within the integrated cloud platforms plotted in the chart, underlining the urgency to utilize AI to detect such attacks. Toppling the chart comes fraud at 4,500 occurrences, cyber harassment with 3,500 occurrences, followed by system vulnerability with 2,500 instances. Also trending are intrusions at 2,200 occurrences, spam with 1,500 occurrences, and malicious code attacks. Fraud and harassment predominate content-related threats to the tune of 1,000 incidents. Intrusion attempts and denial-of-service (DoS) attacks are less prevalent at 800 and 400 instances. Such a distribution speaks volumes about the fact that harassment and fraud characterize cloud security concerns, necessitating smarter detection and mitigation strategies. Deep learning will be essential for examining massive amounts of data flows, detecting nuanced patterns, and evolving response mechanisms to anticipate emerging threats. Through automating threat categorization and prioritizing high-risk attacks such as fraud and intrusion, AI improves protection in real-time. These insights enable guided defence strategies, securing dynamic cloud environments against sophisticated cyber threats.

Figure 11 presents key parameters distinguishing normal and anomalous data samples within integrated cloud platforms for AI-driven threat detection. Normal traffic features a packet size of 500 bytes, IP address 192.168.1.1, port 443, low login attempts (5), and minimal system resource usage (15%). Conversely, anomalous data presents obvious deviations: greater packet sizes (2,500 bytes), unusual IP (10.0.0.1), port 22 (usually attacked in SSH attacks), excessive login attempts (30), and high resource usage (80%). These features are important in detecting threats such as brute force attacks, unauthorized access, and system exploitation. The data set covers different volumes: 50 GB for packet, 30 GB for IP, and up to 80 GB for timestamp, attesting to the size processed by cloud infrastructures. Deep learning algorithms process such patterns of behaviour to identify anomalies in real time, providing accurate, scalable security solutions that evolve with changing cyber threats in cloud-based environments.

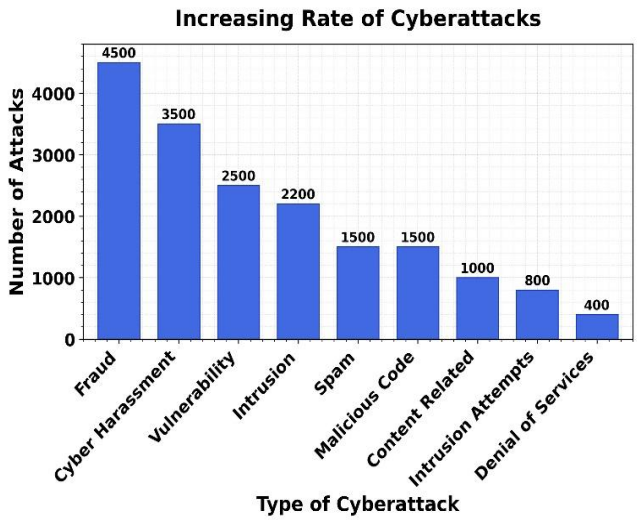

Figure 10. Attack distribution in cloud security

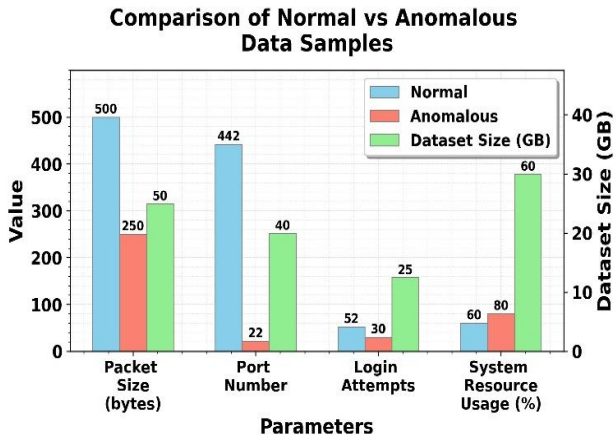

Figure 11. Data patterns in threat detection

Figure 12 analyzes attack types based on normal and anomalous behaviour instances in integrated cloud platforms using AI-driven threat detection. Brute force attacks have the highest data volume, with 270 total points, including 70

anomalies highlighting frequent unauthorised login attempts. DDoS attacks follow with 230 data points and a significant 80 anomalies, indicating disruptive traffic floods. Phishing attempts and insider threats also present substantial anomaly counts (60 and 40, respectively), underscoring challenges in identifying deceptive access and internal misuse. Malware and ransomware, though smaller in volume, show notable anomaly ratios of 50 of 150 and 55 of 145, respectively, suggesting stealthy but impactful behaviour. This distribution emphasises the need for adaptive AI systems to distinguish normal from suspicious activity across diverse attack vectors. Deep learning models enhance detection by learning behaviour patterns, enabling timely, accurate threat responses in complex, data-rich cloud environments. Effective anomaly recognition is critical for maintaining cloud security resilience.

Figure 13 compares the performance of an original deep learning model and various MHWOA-optimised versions in AI-driven threat detection on integrated cloud platforms. The baseline model attains an accuracy of 85% with a high false positive ratio of 10%, computational cost of 250 ms, and response time of 5 s based on a 50 GB dataset. The MHWOA-based optimized model greatly improves detection precision to 92%, decreases false positives to 5%, and decreases computational cost and response time to 180 ms and 3 s, respectively. With an increased dataset (200 GB), the optimized model increases accuracy further to 94% with efficiency. In real-time, it provides 90% accuracy, the minimum false positive (3%), and the maximum response time (2.5 s). These enhancements show MHWOA's capability in increasing model performance, scalability, and real-time responsiveness, and it is extremely applicable for dynamic cloud-based cybersecurity environments.

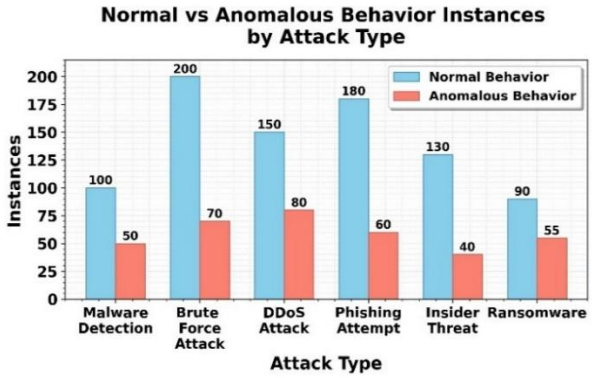

Figure 12. Behavioural patterns in cyber attacks

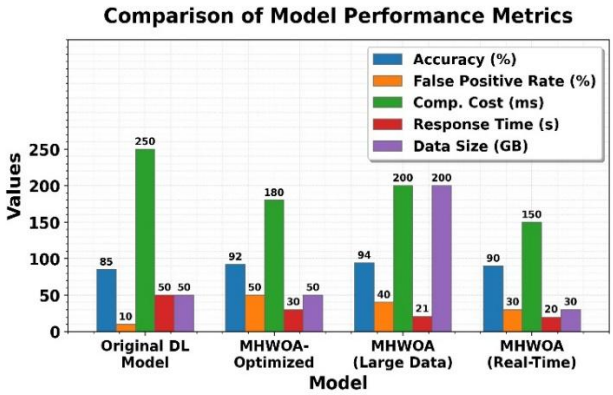

Figure 13. The Multi-Strategy Hybrid Whale Optimization Algorithm (MHWOA) model enhances threat detection

Figure 14 compares the effectiveness of different AI techniques in threat detection within integrated cloud platforms. CABA achieves 88% detection accuracy with moderate response time (4.5 s) and 80% incident response automation. EA-TCN outperforms CABA with 91% accuracy, faster response (3s), and higher automation (85%). When both models are integrated (EA-TCN + CABA), performance peaks: threat detection accuracy reaches 95%, anomaly detection climbs to 94%, and response time drops to 2.5 s. This combined approach also processes the largest data volume (150 GB), highlighting its scalability. The real-time EA-TCN model prioritizes speed, delivering the fastest response (2 s) with 93% accuracy and 95% automation on 40 GB of data. Overall, the integrated EA-TCN + CABA model demonstrates the best balance of precision, efficiency, and scalability, showcasing the critical role of hybrid AI techniques in real-time cyber threat detection and mitigation in cloud environments.

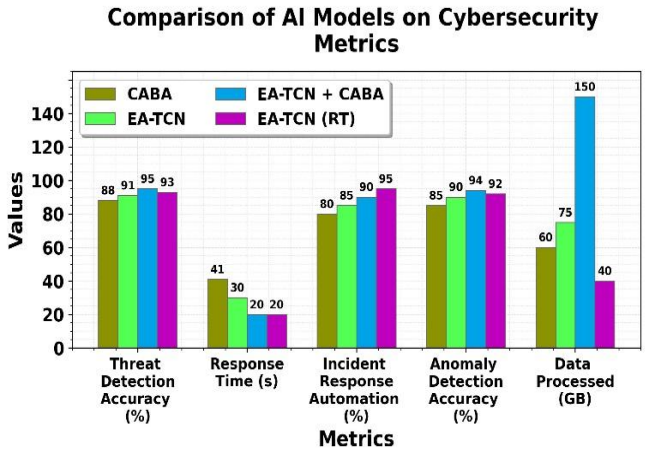

Figure 14. Enhanced AI models for cybersecurity

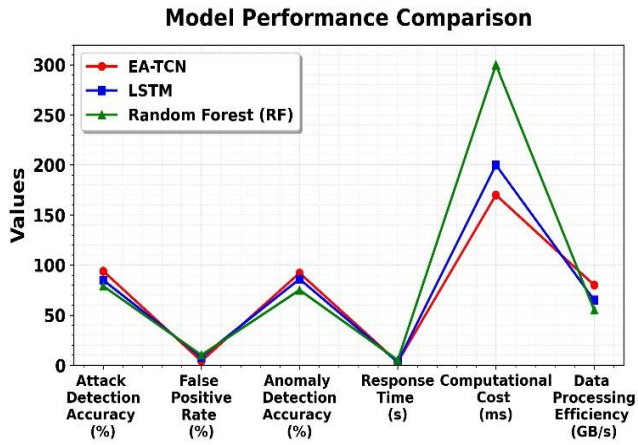

Figure 15. Deep learning in cloud threat detection

Figure 15 shows EA-TCN, LSTM, and RF across key performance metrics for AI-driven threat detection in integrated cloud platforms. EA-TCN significantly outperforms both LSTM and RF in attack and anomaly detection accuracy, achieving 94% and 92%, respectively. It also has the lowest false positive rate at 3%, increasing reliability. On system responsiveness, EA-TCN has the lowest response time (1.8 s) and lowest computational cost (170 ms), showing that it is well-suited to real-time applications. It also leads to data processing efficiency, capable of processing 80

GB/s, compared with LSTM's 65 GB/s and RF's 55 GB/s. LSTM performs moderately across all metrics but lags in speed and accuracy. RF demonstrates the lowest performance, especially with a 10% false positive rate and the slowest response. Overall, EA-TCN is best suited for efficient and accurate cyber-attack mitigation in cloud environments.

The greater performance of EA-TCN is attributed to its capability to capture long-term temporal dependences using dilated causal convolutions, permitting it to sense sequential attack patterns in network traffic. Also, the attention mechanism qualifies the model to focus on critical time intervals related to malicious activity, refining detection sensitivity. MHWOA increases performance by augmenting hyperparameters and choosing the most applicable features, decreasing convergence time and improving organization accuracy. Similarly, SABiW progresses signal value by eliminating noise from raw network data, which significantly diminishes false positive rates. CABA contributes by integrating contextual user behaviour, enabling the system to differentiate between legitimate and irregular actions more efficiently in dynamic cloud environments.

5. CONCLUSION

The research demonstrates that integrated cloud platforms enhanced with deep learning offer a powerful and scalable solution for AI-driven threat detection and cyber-attack mitigation. The proposed hybrid CNN-LSTM model effectively identifies and responds to a wide range of threats, including DDoS and intrusion attempts, with high accuracy and low false positive rates. The incorporation of explainable AI further ensures transparency and trust in the system's decisions, which is critical for cybersecurity operations. The cloud-based deployment enables real-time monitoring, automated response, and centralized data analysis, making it suitable for dynamic and distributed environments. However, the study also highlights challenges such as the need for high-quality datasets and efficient processing architectures. The result indicates EA-TCN outperforms LSTM and RF in attack detection accuracy (94% vs. 92%), the lowest false positive rate (3%), the lowest response time (1.8s), and data processing efficiency (80 GB/s), making it ideal for real-time applications and implemented by using Python Software. Future research should focus on enhancing dataset diversity, improving model generalization, and integrating cross-platform intelligence sharing. Overall, this work confirms that deep learning, when integrated with cloud infrastructure, significantly advances proactive and adaptive cyber defence capabilities.

REFERENCES

[1] Akinbolaji, T.J. (2023). Advanced integration of artificial intelligence and machine learning for real-time threat detection in cloud computing environments. Iconic Research and Engineering Journals, 6(10): 980-991. https://doi.org/10.5281/zenodo.13963676

[2] Gnanasekaran, A., Chinnasamy, A.A, Parasuraman, E. (2022). Analyzing the QoS prediction for web service recommendation using time series forecasting with deep learning techniques. Concurrency Computat Pract Exper, 34(28): e7356. https://doi.org/10.1002/cpe.7356

[3] Anvekar, P., Gudnavar, A., Naregal, K., Nagarmunoli, S. (2024). Detection of manipulated multimedia in digital forensics using machine learning. In International Conference on Device Intelligence, Computing and Communication Technologies (DICCT), Dehradun, India, pp. 33-38. https://doi.org/10.1109/DICCT61038.2024.10533016

[4] Asha, K.N., Rajkumar, R. (2023). DCF-MLSTM: A deep security content-based filtering scheme using multiplicative BiLSTM for movie recommendation system. International Journal of System of Systems Engineering, 13(1): 66-82. https://doi.org/10.1504/IJSSE.2023.129059

[5] Dorothy, A.B., Madhavidevi, B., Nachiappan, B., Manikandan, G., Patjoshi, P.K., Sindhuja, M. (2024). AI-Driven threat intelligence in cloud computing detecting and responding to cyber attacks. In 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS), Hassan, India, pp. 1-6. https://doi.org/10.1109/IACIS61494.2024.10721888

[6] Ofili, B.T., Obasuyi, O.T., Erhabor, O.E. (2024). Threat intelligence and predictive analytics in USA cloud security: Mitigating AI-driven cyber threats. International Journal of Engineering Technology Research & Management, 8(11): 631-646.

[7] Ali, A.R.A.R., Saravanan, K., Abirami, B.B., Pandi, V.S., Aroulanandam, V.V., Parthiban, S. (2024). Enhancing cloud security with AI: Developing robust, scalable solutions for threat mitigation and data protection in cloud platforms. In 2024 International Conference on Sustainable Communication Networks and Application (ICSCNA), Theni, India, pp. 614-620, https://doi.org/10.1109/ICSCNA63714.2024.10863942

[8] Darshan B., Prashanth C. (2023). Dual-discriminator conditional generative adversarial network optimized with hybrid momentum search algorithm and Giza Pyramids Construction algorithm for cluster-based routing in WSN assisted IoT. International Journal of Computer Network and Information Security, 15(5): 96-112. https://doi.org/10.5815/ijcnis.2023.05.09

[9] Farzaan, M.A.M, Ghanem, M.C., El-Hajjar, A., Ratnayake, D.N. (2025). AI-powered system for an efficient and effective cyber incidents detection and response in cloud environments. IEEE Transactions on Machine Learning in Communications and Networking. 3: 623-643. https://doi.org/10.1109/TMLCN.2025.3564912

[10] Khan, M.M. (2024). Developing AI-powered intrusion detection system for cloud infrastructure. Journal of Artificial Intelligence, Machine Learning and Data Science, 2(1): 1-9. https://doi.org/10.51219/JAIMLD/mohammed-mustafa-khan/255

[11] Abisoye, A., Akerele, J., Odio, P.E., Collins, A., Babatunde, G.O., Mustapha, S.D. (2025). Using AI and machine learning to predict and mitigate cybersecurity risks in critical infrastructure. International Journal of Engineering Research and Development, 21(2): 205-224.

[12] S., K., S., A.A., A. D.S., Santhosh, L., Raj, M., Ganesan, D. (2024). Crypto AI: Digital nostalgic art generation using GAN and creation of NFT using blockchain. Journal of Emerging Technologies and Innovative Research, 9(7): 217-220.

[13] Nwachukwu, C., Durodola-Tunde, K., Akwiwu-Uzoma, C. (2024). AI-driven anomaly detection in cloud

computing environments. International Journal of Science and Research Archive, 13(2): 692-710
[14] Radhiya Devi, C., Jayanthi, S.K. (2023). DCNMAF: Dilated convolution neural network model with mixed activation functions for image de-noising. International Journal of Intelligent Systems and Applications in Engineering, 11(4s): 552-557.
[15] Awodele, O., Ogbonna, C., Ogu, E.O., Hinmikaiye, J.O., Akinsola, J.E.T. (2024). Characterization and risk assessment of cyber security threats in cloud computing: A comparative evaluation of mitigation techniques. Acadlore Transactions on AI and Machine Learning, 3(2): 106-118. https://doi.org/10.56578/ataiml030204
[16] Mahendar, K., Shivakanth, G. (2025). AI-SCAN: A scalable AI-driven IDS for cyber threat detection in cloud environments. AUTHOREA. https://doi.org/10.22541/au.174491153.30619618/v1
[17] Abuowaida, S., Owida, H.A., Mohammad, S.I.S., Alshdaifat, N., Elsoud, E.A., Alazaidah, R., Vasudevan, A., lshurideh, M.T. (2025). Evidence detection in cloud forensics: Classifying cyber-attacks in IaaS environments using machine learning. Data and Metadata, 4: 699. https://doi.org/10.56294/dm2025699
[18] Baig, M.D., Akram, W., Haq, H.B.U., Rajput, H.Z., Imran, M. (2024). Optimizing misinformation control: A cloud-enhanced machine learning approach. Information Dynamics and Applications, 3(1): 1-11. https://doi.org/10.56578/ida030101
[19] Priyadarshini, S., Sawant, T.N., Bhimrao Yadav, G., Premalatha, J., Pawar, S.R. (2024). Enhancing security and scalability by AI/ML workload optimization in the cloud. Cluster Computing, 27: 13455-13469. https://doi.org/10.1007/s10586-024-04641-x
[20] Puttaswamy, N.G., Murthy, A.N., Degha, H. (2024). A comparative review of Internet of Things model workload distribution techniques in fog computing networks. Information Dynamics and Applications, 3(1): 21-46. https://doi.org/10.56578/ida030103
[21] Muthusamy, K. (2025). AI-powered threat detection in cybersecurity infrastructures. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 6(1): 23-30. https://doi.org/10.63282/3050-9262.IJAIDSML-V6I1P103
[22] Samson, T.K. (2024). Comparative analysis of machine learning algorithms for daily cryptocurrency price prediction. Information Dynamics and Applications, 3(1): 64-76. https://doi.org/10.56578/ida030105
[23] Shaffi, S.M., Vengathattil, S., Sidhick, J.N., Vijayan, R. (2025). AI-driven security in cloud computing: Enhancing threat detection, automated response, and cyber resilience. ArXiv preprint arXiv: 2505.03945. https://doi.org/10.48550/arXiv.2505.03945
[24] Arif, M.H., Rabby, H.R., Nadia, N.Y., Tanvir, M.I.M., Al Masum, A. (2025). AI-driven risk assessment in national security projects: Investigating machine learning models to predict and mitigate risks in defense and critical infrastructure projects. Journal of Computer Science and Technology Studies, 7(2): 71-85. https://doi.org/10.32996/jcsts.2025.7.2.6
[25] Sharma, P., Prasad, J.S., Shaheen, Ahamed, S.K. (2024). An efficient cyber threat prediction using a novel artificial intelligence technique. Multimed Tools Appl, 83: 66757-66773. https://doi.org/10.1007/s11042-024-18169-0
[26] Azar, A.T., Amin, S.U., Majeed, M.A., Al-Khayyat, A., Kasim, I. (2024). Cloud-cyber physical systems: Enhanced metaheuristics with hierarchical deep learning-based cyberattack detection. Engineering, Technology & Applied Science Research, 14(6): 17572-17583. https://doi.org/10.48084/etasr.8286
[27] Talati, D.V. (2024). AI-powered cloud security: Using user behavior analysis to achieve efficient threat detection. International Journal of Innovative Research in Science, Engineering and Technology, 13(5): 10124-10131. https://doi.org/10.15680/IJIRSET.2024.1305590
[28] Sundaramurthy, S.K., Ravichandran, N., Inaganti, A.C., Muppalaneni, R. (2025). AI-driven threat detection: Leveraging machine learning for real-time cybersecurity in cloud environments. Artificial Intelligence and Machine Learning Review, 6(1): 23-43. https://doi.org/10.69987/AIMLR.2025.60104
[29] Wada, I., Izibili, G.O., Babayemi, T., Abdulkareem, A., Macaulay, O.M., Emadoye, A. (2025). AI-driven cybersecurity in higher education: A systematic review and model evaluation for enhanced threat detection and incident response. World Journal of Advanced Research and Reviews, 25(3): 2233-2245. https://doi.org/10.30574/wjarr.2025.25.3.0989
[30] Ali, G., Shah, S., ElAffendi, M. (2025). Enhancing cybersecurity incident response: AI-driven optimization for strengthened advanced persistent threat detection. Results in Engineering, 25: 104078. https://doi.org/10.1016/j.rineng.2025.104078
[31] Kavitha, D., Thejas, S. (2024). AI enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation. IEEE Access, 12: 173127-173136, 2024, https://doi.org/10.1109/ACCESS.2024.3493957
[32] Alshingiti, Z., Alaqel, R., Al-Muhtadi, J., Haq, Q.E.U., Saleem, K., Faheem, M.H. (2023). A deep learning-based phishing detection system using CNN, LSTM, and LSTM-CNN. Electronics, 12(1): 232. https://doi.org/10.3390/electronics12010232
[33] Vajrobol, V., Gupta, B.B., Gaurav, A. (2024). Mutual information based logistic regression for phishing URL detection. Cyber Security and Applications, 2: 100044. https://doi.org/10.1016/j.csa.2024.100044