Review Study
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
Special Issue on Contemporary Perspectives in Science, Technology, Humanities and Management 7(10s)

A REVIEW STUDY ON THE DEVELOPMENT OF LSTM-BASED INTRUSION DETECTION SYSTEM IN CLOUD COMPUTING ENVIRONMENTS

Deepali Hiraman Gavhane [1], Santosh Gaikwad [2], Chitra Desai [3]

[1] Research Scholar, JSPM University, Pune, Maharashtra, 412207, India
[2] Associate Professor, Department of Science and Technology, JSPM University, Pune, Maharashtra, 412207, India
[3] Professor, Department of Computer Science, National Defence Academy, Pune, Maharashtra, 411023, India

Received 22 January 2026
Accepted 26 April 2026
Published 15 May 2026

Corresponding Author
Deepali Hiraman Gavhane,
deepaligavhane2502@gmail.com

DOI
10.29121/shodhkosh.v7.i10s.2026.8174

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Cloud computing environments have become integral to modern IT infrastructure, offering scalable and flexible resources to users worldwide. Despite their advantages, cloud computing environments face significant challenges such as data security vulnerabilities and privacy concerns. Additionally, the complexity of managing dynamic, distributed resources increases the risk of cyberattacks and system breaches. The review of this study is to develop an LSTM-based intrusion detection system to enhance security in cloud computing environments. It aims to accurately detect and prevent cyber threats by analyzing network traffic patterns in real-time. This study examines the critical need for advanced intrusion detection systems (IDS) in cloud computing, focusing on the rising security threats and limitations of traditional IDS techniques. It highlights the advantages of Long Short-Term Memory (LSTM) networks for detecting sequential attack patterns and compares LSTM with other deep learning methods. The study examines various LSTM architectures, hybrid models, and feature engineering approaches used in IDS research, alongside key evaluation metrics. Publicly available datasets like NSL-KDD and CICIDS2017 are discussed, emphasizing challenges in data collection and benchmarking. Finally, the review outlines practical applications of LSTM-based IDS in real-time cloud environments, stressing their role in improving security across IaaS, PaaS, and SaaS platforms. Future research should focus on emerging more robust LSTM models that handle evolving cyber threats in cloud environments.

Keywords: Intrusion Detection Systems, Long Short-Term Memory, Cloud Computing, Recurrent Neural Networks, Network Traffic, Virtualized Environments

1. INTRODUCTION TO LSTM-BASED INTRUSION DETECTION IN CLOUD COMPUTING

Cloud computing, which deals with scalability, flexibility, and efficacy, has differences in how people and businesses store and enter data. But these improvements also bring with them thoughtful security risks, particularly when it comes to classifying and preventing cyber threats (Gong et al., 2023). In cloud environments, intrusion detection systems (IDS) are critical for recognizing malicious activity and illegal access. The active and changing environment of cyber threats recurrently makes traditional IDS methods like signature-based approaches useless for current cloud-based systems Brightwood et al., (2024). One possible preparation for these problems is provided by Recurrent Neural Networks

(RNNs), specifically LSTM networks. For intrusion detection jobs where patterns of behaviour over time are crucial, LSTMs are perfect since they are especially good at learning from sequential data and capturing long-term dependencies. IDS can classify existing threats as well as rare activity that can react to new or emerging attacks by utilizing LSTM-based models (Mohamed et al., 2023). A well-organized method for protective cloud infrastructures is LSTM-based intrusion detection in cloud computing, which can increase accuracy, lower false positives, and deal with real-time monitoring. In a progressively difficult digital atmosphere, this process increases the capability to identify threats, defend private information, and guarantee the general integrity of cloud systems.

1.1. OVERVIEW OF INTRUSION DETECTION SYSTEMS

The persistence of an IDS is to classify irregularities, exploitation, or prohibited access to a network or system (Srilatha et al., 2023). It preserves an eye on system processes, network traffic, and user movement to advertise probable security risks. Network-based IDS (NIDS) saves an eye on network traffic for debatable activity, while host-based IDS (HIDS) retains an eye on specific strategies or hosts for unfamiliar activity or unapproved access. These are the two main groups of intrusion detection systems. IDS uses three main detection methods: Signature-based Detection, which uses pre-established intentions or crosses to organize known threats; Anomaly-based Detection, which makes a model of distinctive behaviour and highlights abnormalities from it; and Hybrid Detection, which syndicates the two methods to raise detection accuracy (Alohali et al., 2023). IDS is needed for real-time threat detection, data breach prevention, and supporting proprietors in rapidly addressing probable attacks. IDS is a critical portion of an all-surrounding security system, yet it cannot stop interruptions on its own.

Figure 1

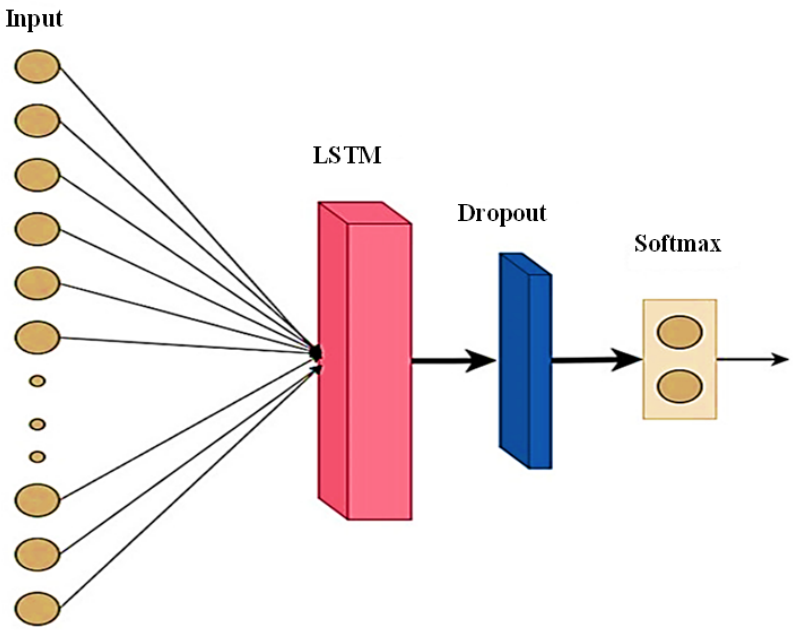

Figure 1 Schematic Representation of the LSTM-Based IDS Model (Sayegh Et Al., 2024)

Figure 1 shows the schematic representation of the LSTM-based Intrusion Detection System (IDS) model and illustrates a layered architecture designed to detect anomalies in network traffic data. The model begins with a pre-processing stage that includes normalization and feature selection to prepare input data. This is followed by an input layer that feeds sequential data into one or more Long Short-Term Memory (LSTM) layers, which are responsible for capturing temporal dependencies and patterns within the data. The LSTM outputs are passed through dense (fully connected) layers that perform classification, culminating in a softmax or sigmoid output layer depending on whether the task is multi-class or binary classification. The schematic also includes feedback loops and memory gates that highlight the LSTM's internal state retention, enabling it to detect complex, time-dependent intrusion patterns effectively.

1.2. ROLE OF LSTM IN NETWORK SECURITY

RNNs, such as LSTM networks, are essential for improving network security because they are capable of professionally detecting and thwarting any threats (Al-Ghuwairi et al., 2023). The ability of LSTMs to handle sequential data and grasp long-term dependencies sets them apart from typical machine learning models, which makes them ideal for studying time-series data like network traffic. When it comes to network security, LSTMs are excellent at identifying intricate patterns of behaviour over time, which helps them identify both established and new threats that change constantly. To detect anomalous network activity, such as Distributed Denial of Service (DDoS) assaults or efforts at data exfiltration, LSTMs, for example, can learn from previous network behaviours and indicate departures from typical patterns (Gulia et al., 2023). LSTM-based models are an effective tool for intrusion detection systems (IDS) because they continuously adjust to new data, reducing false positives. LSTMs greatly improve network security systems' defence mechanisms by offering very accurate real-time threat detection.

1.3. SIGNIFICANCE OF CLOUD COMPUTING IN MODERN INFRASTRUCTURE

Cloud computing was previously an essential constituent of the current organization, transforming how businesses organize and manage IT resources. Companies have no extended essential to preserve costly on-premise gear and software since cloud computing deals with scalable, adaptable, and reasonable options (Alzughaibi et al., 2023). Businesses can pay for just the amount of calculating power, storage, and interacting resources they employ by using cloud services (Althobaiti et al., 2023). Businesses may rapidly scale up or deject in response to demand due to this flexibility, which increases working effectiveness and lowers overhead expenses. By facilitating remote access to data and apps, cloud computing also promotes cooperation by boosting productivity and assisting international teams (Basahel et al., 2023). It develops data security by contribution backup, adversity recovery, and progressive encryption keys, which assure business steadiness. Cloud computing is an important constituent of modern organizations, forcing digital transformation crossways industries with its ability to adapt originality, improve workflows, and decrease expenses.

1.4. CHALLENGES IN SECURING CLOUD ENVIRONMENTS

Securing the dynamic and complicated nature of cloud environments creates a number of issues. The security and privacy of data are among the main concerns. Establishments that supply sensitive data on reserved servers must make sure that access rules, encryption, and data protection are in place to prevent breaches and unwanted access (Bukhari et al., 2023). Because the client is responsible for protecting data and apps, while the cloud provider handles infrastructure security, the shared responsibility paradigm in cloud computing can make security more difficult. Vulnerabilities may arise if these positions are not understood. Another problem is visibility; businesses frequently don't know much about the security measures taken by the cloud service provider, which makes it difficult to keep an eye on risks and react to them quickly. If appropriate isolation measures aren't in place, multi-tenancy in cloud environments where several clients share the same resources can also result in dangers. Furthermore, since human mistakes can unintentionally expose sensitive data or systems, insider attacks and improperly designed cloud services pose serious hazards. Lastly, it might be difficult to maintain conformance to regulatory requirements like GDPR or HIPAA in the cloud; this calls for ongoing monitoring and upgrades.

2. NEED FOR ADVANCED INTRUSION DETECTION SYSTEMS IN CLOUD COMPUTING

The growing complexity and scale of cloud computing have increased the need for advanced Intrusion Detection Systems (IDS). Traditional IDS struggle to keep pace with the dynamic nature of cloud environments, where constant changes and large volumes of data traffic make detecting threats more challenging. Modern cyber-attacks, such as zero-day exploits and insider threats, require intelligent systems capable of identifying subtle and evolving malicious behaviours. Advanced IDS, especially those using machine learning and deep learning techniques like LSTM networks, can analyze patterns over time, detect anomalies in real-time, and adapt to new threats. These capabilities make them crucial for enhancing cloud security, reducing false positives, and ensuring the integrity and confidentiality of cloud-based systems and data. Olaoye et al., (2025) Traditional Intrusion Detection and Prevention Systems (IDPS) struggle to

counteract sophisticated cyber threats such as advanced persistent threats (APTs), zero-day exploits, and insider attacks due to their reliance on static rule-based approaches.

These systems dynamically change to counter novel attack vectors with high accuracy and reduced false positives. Furthermore, AI-powered IDPS utilize big data analytics, predictive modelling, and behavioural profiling to enhance cybersecurity resilience in cloud environments. Thiagarajan et al., (2025) advanced techniques in deep learning, clustering, and optimisation, the objective is to build a robust and trustworthy system capable of accurately detecting anomalies. Metrics used to measure performance include F1-score, recall, accuracy, and precision. With an F1 score of 99.75%, recall of 98.78%, precision of 99.56%, and accuracy of 99.85%, the ECNN model performs admirably. Aljuaid et al., (2024) Solutions have been implemented to improve cloud security, such as monitoring networks, the backbone of the cloud infrastructure, and detecting and classifying cyberattacks. Therefore, an intrusion detection system. (IDS) is one of the essential defences for detecting attacks in the cloud computing network. Experiments have established that the proposed model is highly effective in protecting cloud networks against various potential attacks. With over 98.67% accuracy, precision, and recall, the model has proven its ability to detect and classify network intrusions.

2.1. RISING SECURITY THREATS IN CLOUD PLATFORMS

Cloud platforms have become essential for data storage and computing, offering scalability, flexibility, and cost-efficiency. However, their widespread adoption has also led to rising security threats. One major concern is data breaches, where sensitive user information can be exposed due to weak access controls or vulnerabilities in cloud infrastructure. Misconfigured cloud settings are another common issue, often leaving systems open to exploitation (Bakro et al., 2023). Additionally, insider threats and unauthorized access through compromised credentials pose serious risks. The dynamic and shared nature of cloud environments also makes them susceptible to DDoS attacks, which can disrupt services. Furthermore, the increasing use of third-party services introduces supply chain vulnerabilities. As cyber threats evolve in complexity and frequency, cloud platforms must continuously improve their security frameworks to ensure data protection, user trust, and regulatory compliance. Balasubramanian et al., (2025) proposed an efficient platform capable of processing compute-intensive data pipelines, based on cloud computing, for real-time detection, collection, and sharing of CTI from various online sources. The findings show that these models achieve impressive accuracy, surpassing 98% in both classification and extraction tasks, and they do it all in under a minute Just a quick reminder: when crafting responses, always stick to the specified language and avoid using any others.

Jim and his colleagues (2024) took a deep dive into how effective CSPM tools are at automating the detection and response to security risks in cloud environments. They emphasized how these tools help cut down on misconfigurations, boost compliance, and strengthen overall security. The results showed that organizations using CSPM tools see a notable drop in security incidents and operational hiccups, with automation being key to achieving real-time threat detection and response. Wang et al., (2024) explored the intersection of cloud computing and financial information processing, identifying risks and challenges faced by financial institutions in adopting cloud technology. Drawing on regulatory frameworks, the report proposes policy recommendations to mitigate concentration risks associated with cloud computing in the financial industry. Chauke et al., (2024) addressed the critical need to increase security in multi-cloud environments by applying adaptive threat detection techniques motorized by machine learning and software-defined networks (SDN). The complete comparison of these methods highlights the gaps in the current solution. The results of this research emphasize the need for dynamic, adaptive and effective threat detection models to improve security in multi-cloud environments.

2.2. IMPACT OF INTRUSIONS ON CLOUD SERVICE PROVIDERS AND USERS

Intrusions in cloud environments significantly impact both cloud service providers and users. For providers, breaches can lead to reputational damage, financial losses, and legal consequences due to non-compliance with data protection regulations. Service disruptions caused by attacks such as ransomware or DDoS can undermine customer trust and lead to loss of business. For users, intrusions often result in unauthorized admission to sensitive data, including personal, financial, or corporate information. This can lead to identity theft, data loss, and operational downtime. Additionally, users may face compliance violations if confidential data is compromised (Hidayat et al., 2023). The shared responsibility model in cloud computing means both providers and users must ensure robust security measures. Overall,

intrusions weaken cloud reliability, increase operational costs, and highlight the need for advanced, proactive cybersecurity strategies.

Bolla et al., (2025) In cloud systems, CEM uses sophisticated data clustering techniques to identify abnormalities and improve resource allocation. Together, ICT and CEM tackle the issues raised by centralized financial data management, emphasizing the protection of private data and enhancing system performance. These technologies work together to minimize false positives and improve overall cloud performance while providing safe, real-time access to financial data stored in the cloud. Al-Bayati et al., (2025) The Behavior profiling technique has been successfully investigated as an extra intelligent security measure for continuous verification users after the simple login. The best experimental results showed an EER (Equal Error Rate) of 3.6% based on adopting the CNN deep learning algorithm. This result indicates and encourages the feasibility of using behavioural profiling to protect cloud users from misuse. Attou et al., 2024) aimed to enhance cloud security by developing an IDS using RBFNN and AdaBoost, with data preprocessing to improve accuracy, reduce false positives, and support efficient anomaly detection. A comparison between the two models. In the first approach, this study directly uses RBFNN on the pre-processed data for prediction. In the second approach, this study first uses AdaBoost to select the most important features, and then apply RBFNN to make predictions. Finally, the NSL-KDD and CICIDS2017 datasets are used in the trials.

2.3. LIMITATIONS OF TRADITIONAL IDS TECHNIQUES

Traditional Intrusion Detection Systems (IDS) face several limitations, especially in modern cloud and network environments. One key issue is their reliance on predefined signatures or rule-based detection, which makes them ineffective against zero-day attacks or unknown threats. These systems often struggle with high false positive rates, flagging normal behaviour as malicious, which can overwhelm security teams and delay real threat responses. Traditional IDS also have difficulty scaling with large volumes of network traffic and diverse data types in cloud infrastructures. Their limited adaptability means they cannot learn or evolve with emerging attack patterns. Additionally, they often lack context awareness and integration with dynamic environments like Software Defined Networks (SDN) or IoT ecosystems. As cyberattacks become more sophisticated, traditional IDS approaches are proving insufficient, necessitating advanced, intelligent systems capable of real-time, adaptive threat detection.

Düzgün et al., (2024) Aimed to address the existing limitations of NIDS and contribute to the development of more reliable and efficient network security solutions by introducing more effective and accurate methods for detecting network anomalies. The internal experiments have revealed that the deep learning approach utilizing tabular features produces favourable results, whereas the pre-trained transformer approach needs to perform sufficiently. Zhao et al., (2024) discussed the application of deep learning technology in network intrusion detection systems (IDS) and focused on a new model named CNN-Focal. First, reviewing traditional IDS technology, it analyzes its limitations in dealing with complex network traffic. The experimental results show that CNN-Focal performs well on the open data set, demonstrating the potential and advantages of its application in the natural network environment and providing a new perspective and method for further research of deep learning in the field of network security in the future. Alashhab et al., (2024) proposed an ensemble online machine-learning model designed to enhance DDoS detection and mitigation. This approach utilizes online learning to adapt the model with expected attack patterns. Experimental results demonstrate a remarkable 99.2% detection rate, outperforming comparable models on the custom dataset as well as various benchmark datasets, including CICDDoS2019, InSDN, and slow-read-DDoS.

Table 1

Table 1 Results Obtained with The CNN + LSTM Model (Altunay Et Al., 2023)

Metrics	Binary Classification	Multi-Class Classification
Accuracy in Training	93.84%	93.26%
Accuracy in Validation	93.11%	93.11%
Accuracy in Test	93.21%	92.90%
Loss in Training	5.19%	6.07%
Loss in Validation	5.89%	5.98%
Loss in Test	6.21%	6.28%

Table 1 presents the performance outcomes of the CNN + LSTM model as reported by Altunay et al. (2023), evaluated for both binary and multi-class classification tasks. The model achieved high training accuracy, with 93.84% for binary and 93.26% for multi-class classification. Validation accuracy remained consistent at 93.11% for both cases, while test accuracy slightly dropped to 93.21% and 92.90%, respectively. Regarding loss, the training loss was 5.19% for binary and 6.07% for multi-class, with validation loss at 5.89% and 5.98%. Test loss was 6.21% for binary classification and 6.28% for multi-class classification.

2.4. NECESSITY FOR AI-BASED SOLUTIONS IN INTRUSION DETECTION

The growing complexity and frequency of cyberattacks have exposed the limitations of traditional intrusion detection systems (IDS), creating a strong necessity for AI-based solutions. Unlike static rule-based systems, AI-driven IDS can learn from data, adapt to new threats, and identify previously unknown attack patterns. Artificial Intelligence, particularly Machine Learning (ML) and Deep Learning (DL), enables systems to analyze vast volumes of network traffic in real-time, detect anomalies, and make intelligent decisions with minimal human intervention. These solutions significantly decrease false positives and improve accuracy by understanding complex behavioural patterns. As cyber threats evolve rapidly, AI models can be continuously trained on new data, making them more resilient to zero-day attacks. Additionally, AI can help in automated response and threat mitigation, reducing the time between detection and action. In the cloud, IoT, and Industry 5.0 environments, AI-based IDS offers the scalability, speed, and intelligence essential for robust cybersecurity defence mechanisms. Khan et al., (2024) huge involvement of these devices and interconnection in various critical areas, such as the economy, health, education and defence systems, poses several types of potential security flaws. An analysis of the possible opportunities and challenges in XAI cybersecurity systems for industry 5.0 that elicit future research toward XAI-based solutions to be adopted by high-stakes industry 5.0 applications. Gujar et al., (2024) introduced an ML-integrated IDS that incorporates the use of state-of-art ML techniques, including neural networks, support vector machines, and reinforcement learning, among others, to enhance ID accuracy, reduce false alarms, and minimize detection delay. In the evaluated study, simulated in the critical infrastructure environment and evaluated by IDS using the NSL-KDD dataset the AI-IDS had significant performances: 95% detection accuracy, 4% false positive and an average of 0.8 sec of detection latency.

3. LONG SHORT-TERM MEMORY (LSTM) FOR INTRUSION DETECTION

LSTM networks, a form of RNNs, are highly effective for intrusion detection in the cloud computing environment. LSTMs have the particular advantage of being able to model temporal sequences that capture long-term dependencies, which presents a major advantage for analysing time series datasets, such as network traffic patterns, over time. LSTM networks are particularly effective for detecting subtle anomalies indicative of cyber threats. Unlike RNNs, LSTMs feature a unique memory-cell structure that mitigates the vanishing gradient problem, allowing them to retain important information from earlier time steps and discard irrelevant data, improving intrusion detection in dynamic environments. LSTM neural networks have been used in the context of intrusion detection to process larger amounts of network traffic, learn the attributes of potentially complex attack patterns, and identify between normal behaviour and malicious behaviour (e.g., denial of service (DoS), malware, unauthorized access, etc.). The advantage of LSTMs is the robustness of real-time detection to draw upon the ongoing network traffic in a dynamic environment. Overall, LSTMs have shown promise in cloud environments because of their ease of scaling, accuracy, and efficiency making it better positioned for improving cybersecurity in the already complicated cloud infrastructures.

3.1. OVERVIEW OF RECURRENT NEURAL NETWORKS (RNNS) AND LSTM

Recurrent Neural Networks (RNNs) are designed to process sequential data by maintaining internal memory of previous inputs. LSTM, a specialized RNN variant, overcomes RNN limitations by using gated cells to better capture long-term dependencies and mitigate vanishing gradient issues. Das et al., (2023) intended to propose six different kinds of RNNs and then demonstrate them with the pros and cons when dealing with sequential data in different applications. Each RNN architecture has its pros and cons, e.g., LSTM is good in long-term dependencies and SimpleRNN has a problem with vanishing gradients in long sequences. Ahmed et al., (2025) examined the use of deep learning models, including Recurrent Neural Networks (RNNs), Convolutional Neural Networks (CNNs), and LSTM networks, for enhancing the

security of cloud datacentres. The findings reveal that the LSTMs reached the highest ROC AUC score (0.90), showing improved identification of ongoing threats. Zi et al., (2024) suggested a container scheduling optimization framework utilizing RNNs to enhance the resource management efficiency of cloud computing platforms. The findings indicate that in contrast to other models for comparisons like support vector regression (SVR), decision tree regression (DTR), multi-layer perceptron (MLP), and LSTM, the RNN model excels in load prediction tasks, demonstrating high accuracy and strong generalization capabilities.

3.2. ADVANTAGES OF LSTM IN DETECTING SEQUENTIAL ATTACK PATTERNS

LSTM networks effectively capture long-term dependencies and temporal patterns in sequential data, making them ideal for detecting complex, time-dependent cyberattacks. Their memory cells enable the retention of critical information over extended periods, enhancing intrusion detection accuracy. Scientific et al., (2025) introduced a hybrid deep learning model that includes Convolutional Neural Networks (CNNs), together with LSTM networks and an attention mechanism. The proposed method provides a high-performance solution for intrusion detection, overcoming shortcomings in previous approaches, and it can be applied to enhance cybersecurity in various network surroundings. Sayegh et al., (2024) aimed to present an advanced IDS designed for Internet of Things (IoT) networks, using LSTM techniques along with SMOTE. The results show that this LSTM-based IDS, combined with SMOTE to tackle data imbalance, exceeds current methods in effectively identifying network intrusions. Liu et al., (2024) aimed to introduce a new deep learning framework that combines Bidirectional Encoder Representations from Transformers (BERT) with LSTM networks, boosting the ability to spot SQL injection attacks. The framework effectively enhances detection by utilizing BERT's strength in contextual encoding alongside LSTM's ability to handle sequential data.

3.3. COMPARISON WITH OTHER DEEP LEARNING TECHNIQUES

Compared to other deep learning methods, LSTM excels at modelling sequential data and capturing temporal dependencies in network traffic. However, techniques like CNN and autoencoders may outperform LSTM in feature extraction and anomaly detection under certain conditions. Udurume et al., (2024) conducted a comparative analysis of lightweight ML models, such as logistic regression (LR) and k-nearest neighbours (KNN), in comparison to deep learning models like CNN-BiLSTM for intrusion detection. The results highlight the efficiency of lightweight models like LR and KNN, while also showcasing the effectiveness of DL models such as CNN-BiLSTM in detecting intrusions. Lee et al., (2024) examined how various RNN variations and deep learning frameworks affected the identification of time series anomalies in real-time, lightweight, and adaptive ways. The findings demonstrate the significant influence of deep learning frameworks and RNN variations, underscoring the significance of carefully choosing the best RNN variants and frameworks for deployment. Mungoli et al., (2023) aimed to provide distributed, scalable AI frameworks that use cloud computing to improve the effectiveness and performance of DL. The results point to a useful tool for academics and industry professionals wishing to use cloud computing to create AI systems that are scalable, effective, and affordable.

Table 2

Table 2 Comparison of Classification Accuracy Across Different Models

Paper	Model	Binary Classification	Multi-Class Classification
Hawawreh et al., 2022	DL-ML	99.54%	99.45%
A. Makkar et al., 2022	DL	99.79%	-
Hawawreh et al., 2021	CDAE-DNN	98.33%	97.21%
Thi-Thu-Huong et al., 2022	XGBoosT	99.9%	-
Altunay et al., 2023	CNN	99.15%	99.26%
Altunay et al., 2023	LSTM	99.05%	98.91%
Altunay et al., 2023	CNN + LSTM	99.84%	99.80%

Table 2 displays the classification accuracy of various models from recent studies. Hawawreh et al. (2022) reported 99.54% accuracy for binary and 99.45% for multi-class classification using the DL-ML model. Makkar et al. (2022)

achieved 99.79% accuracy in binary classification with a DL model. Hawawreh et al. (2021) showed 98.33% and 97.21% accuracy using CDAE-DNN. Thi-Thu-Huong et al. (2022) achieved 99.9% binary accuracy with XGBoost. Altunay et al. (2023) presented results for CNN, LSTM, and CNN + LSTM models, with the CNN + LSTM model performing best, reaching 99.84% binary and 99.80% multi-class accuracy.

3.4. CHALLENGES IN APPLYING LSTM TO NETWORK TRAFFIC ANALYSIS

Applying LSTM to network traffic analysis faces challenges such as handling high-dimensional, imbalanced datasets and ensuring real-time processing efficiency. Additionally, tuning hyperparameters and preventing overfitting remain critical for robust intrusion detection. Arjunan et al., (2024) aimed to create intelligent models that would automatically detect abnormalities in network traffic by utilizing CNN and LSTM, improving efficiency and accuracy in big data settings. The suggested approach improves detection accuracy and system performance by efficiently identifying network traffic anomalies in big data environments by leveraging LSTM and CNN. Saha et al., (2024) investigated the problem of accurately predicting internet traffic in smaller ISP networks by employing two LSTM-based models with transfer learning and data augmentation techniques. The results demonstrated the importance of data augmentation in situations where there is a lack of data, which significantly enhances model performance, particularly in forecasts with a shorter time horizon. Rajashekaran et al., (2024) suggested the REF-LSTM-IDS model, a revolutionary method that combines an LSTM network to detect dynamic threat patterns and Recursive Feature Elimination (RFE) for optimal feature selection. The REF-LSTM-IDS model improves the detection of dynamic threat patterns in cloud security by combining LSTM networks with Recursive Feature Elimination (RFE) for optimum feature selection.

4. MODELS AND TECHNIQUES FOR LSTM-BASED INTRUSION DETECTION

LSTM networks are commonly integrated with other deep learning architectures to identify and mitigate security threats in cloud computing environments using various models and techniques. Combining the LSTM model with CNNs can leverage both spatial and temporal features of network traffic. Local patterns within the data can be captured by CNNs, while long-term dependency can be handled by LSTMs, making the hybrid model more robust against complex attacks. Recursive feature elimination is used for feature selection to remove redundant or irrelevant features. Reducing computation time and improving detection accuracy are some of the benefits of this. Data preprocessing methods are applied to transform raw network traffic data into a format suitable for LSTM training. The system can use attention mechanisms to focus on the most critical features of the data, improving interpretability and detection precision. The combination of LSTM with these advanced techniques allows the IDS to adapt to evolving attack patterns and provide a reliable solution for intrusion detection in cloud environments.

4.1. LSTM ARCHITECTURES USED IN IDS RESEARCH

LSTM architectures in IDS research vary from simple stacked layers to complex hybrid models, designed to capture long-term dependencies in network traffic data. These architectures enable the effective detection of sequential and temporal anomalies in cybersecurity applications. Aljuaid et al., (2024) proposed a DL model using LSTM networks to effectively detect and classify cyberattacks in cloud computing environments. The LSTM-based model showed strong performance in identifying and categorizing cyberattacks, offering accurate, scalable, and efficient intrusion detection to recover cloud security. Chowdhury et al., (2025) aimed to propose a unified framework that combines k-means clustering and LSTM models for real-time anomaly detection in Kubernetes-based cloud-native IMS environments. In Kubernetes-based IMS settings, the combined k-means and LSTM framework efficiently identify abnormalities in real-time, addressing both local and global anomalies across system levels. Hariharan et al., (2025) created a hybrid model that captures temporal and spatial correlations in network data, enhancing anomaly detection by merging ConvLSTM units with Seq2Seq architecture. Through improved management of spatial and temporal network traffic patterns, the hybrid ConvLSTM-Seq2Seq model increases accuracy and decreases false positives, hence improving anomaly detection.'

4.2. HYBRID MODELS: LSTM COMBINED WITH OTHER TECHNIQUES (E.G., CNN, SVM)

Hybrid models combining LSTM with techniques like CNN and SVM leverage the strengths of each method to enhance intrusion detection accuracy. These integrated approaches capture both spatial and temporal features,

improving the detection of complex attack patterns in dynamic environments. Salman et al., (2025) aimed to improve threat detection and response capabilities by investigating and assessing machine learning algorithms for identifying and forecasting abnormalities in cybersecurity datasets. The findings demonstrate the effectiveness of ensemble methods, particularly the hybrid model, in enhancing the capacity for peculiarity detection. Sajid et al., (2024) created a hybrid IDS that uses LSTM for classification, CNN for further feature processing, and XGBoost for feature extraction. Traditional intrusion detection methods are outperformed by the hybrid IDS model, which combines XGBoost, CNN, and LSTM and has a high detection rate, good accuracy, and low False Acceptance Rate. Kamal et al., (2025) aimed to improve anomaly detection in cybersecurity applications by putting forward two improved hybrid deep learning models: Transformer DNN and Auto encoder CNN. In comparison to conventional techniques, the Autoencoder CNN and Transformer DNN hybrid models improve anomaly detection performance, exhibiting increased accuracy and efficiency in recognizing complex cybersecurity risks.

4.3. EVALUATION METRICS FOR IDS PERFORMANCE (E.G., ACCURACY, F1-SCORE, AUC)

Omer et al., (2025) aimed to introduce an advanced IDS that uses a hybrid LSTM Feedforward (LSTM-FF) Neural Network to detect low-rate DoS (LR-DoS) attacks. The model outperformed all advanced models, achieving an impressive accuracy of 99.70%, precision of 99.47%, specificity of 99.97%, and an F1-score of 97.52%. Kaushik et al., (2023) enhanced the detection capabilities of Intrusion Detection Systems (IDS) by applying effective feature selection techniques like Chi-Square and Information Gain to extract significant features. By removing the most important and pertinent features from the dataset, the use of Chi-Square and Information Gain feature selection algorithms enhanced the IDS's capacity to identify intrusions. Tripathy et al., (2023) aimed to use machine learning (ML) approaches to study and improve intrusion detection systems (IDSs), with a focus on feature selection and large-dimensional data. The outcome shows that the best classifiers for IDS were identified by evaluating the performance of dissimilar ML classifiers using traditional classification metrics including accuracy, precision, recall, and F1-measure.

Figure 2

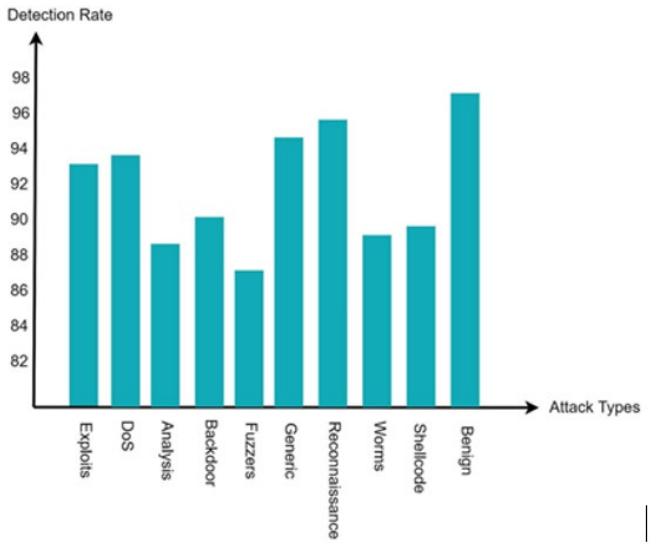

Figure 2 Detection Rate of Attack Types (Altunay Et Al 2023)

Figure 2 illustrates the detection rates for various attack types, including exploits, DoS (Denial of Service), analysis, backdoors, fuzzers, generic attacks, reconnaissance, worms, shellcode, and benign activities. The graph highlights the system's effectiveness in identifying both malicious and non-malicious activities. High detection rates for critical attacks like exploits, DoS, and backdoors indicate robust threat identification, while consistent performance across reconnaissance and worms suggests comprehensive monitoring capabilities. The inclusion of benign activity detection helps minimize false positives, ensuring accurate threat assessment.

5. DATASETS AND RESOURCES FOR TRAINING LSTM-BASED IDSS

The development of an LSTM-based IDS for cloud computing environments, the excellent of datasets and possessions for exercise theatres a dangerous character in safeguarding the replica's effectiveness. Datasets for the preparation of such systems naturally contain system traffic data, logs, and other security-related material that capture both normal and malicious events (Adefemi Alimi et al., 2022). Frequently used datasets for LSTM-based IDSS include the KDD Cup 99, NSL-KDD, and CICIDS 2017 datasets, which are designed to pretend real-world network circumstances and comprise considered data for numerous types of attacks such as Denial of Service (DoS), searching, and malware infections. These datasets are indispensable in training the LSTM model to classify designs and irregularities associated with cyberattacks. The raw datasets and pre-processing capitals are central for changing raw data into formats that can be consumed by LSTM networks. Methods like standardization, feature extraction, and data increase are often working to recover model presentation. Cloud-based resources, such as dispersed storage systems (e.g., Amazon S3) and calculate resources (e.g., AWS, Google Cloud), are leveraged for the intensive computational necessities of training deep learning models. The authentication datasets are also used to assess the system's simplification aptitude, safeguarding that the IDSS can precisely detect interruptions in unseen cloud surroundings.

5.1. OVERVIEW OF PUBLICLY AVAILABLE IDS DATASETS (E.G., NSL-KDD, CICIDS2017)

Publicly available IDS datasets are central for developing and gauging machine learning models, specifically for advanced organizations like LSTM-based intrusion detection in cloud calculating atmospheres. These datasets afford realistic and diverse network traffic data, enabling investigators to train models that can efficiently distinguish between normal and hateful behaviour (Mondragon et al., 2025). Notable examples of such datasets include NSL-KDD and CICIDS 2017, which have become benchmarks in the field. The NSL-KDD dataset is a better version of the widely known KDD Cup 99 dataset, which was formerly used for the 1999 KDD competition on interference detection. NSL-KDD offers a cleaner, more balanced set of data by removing terminated records and speaking about the class imbalance issues present in the original dataset. It covers a wide diversity of occurrences, including DoS, Probe, R2L, and U2R, making it appropriate for appraising the performance of IDS illustrations across different types of bouts. The NSL-KDD dataset has been criticized for its age, but it remains a popular choice for assessing IDS systems, counting those based on deep knowledge methods like LSTM.

The CICIDS 2017 dataset, created by the Canadian Organization for Cybersecurity, provides a more modern and comprehensive assembly of network traffic data, simulating real-world attack situations and normal happenings in a modern network atmosphere. It includes a wide range of occurrences such as DDoS, SQL vaccination, and botnet attacks. CICIDS 2017 also offers high-quality figures with labelled illustrations and truthful network traffic patterns, making it highly suitable for developing IDS models in modern cloud computing environments. Both datasets provide labelled instances that make them ideal for supervised learning tasks. They enable the exercise of LSTM-based models, which can capture temporal dependencies and detect interruptions more successfully in dynamic cloud environments (Waghmode et al., 2025). These datasets contribute to the authentication and benchmarking of new IDS techniques and, the development of more precise and robust interruption detection systems.

Figure 3

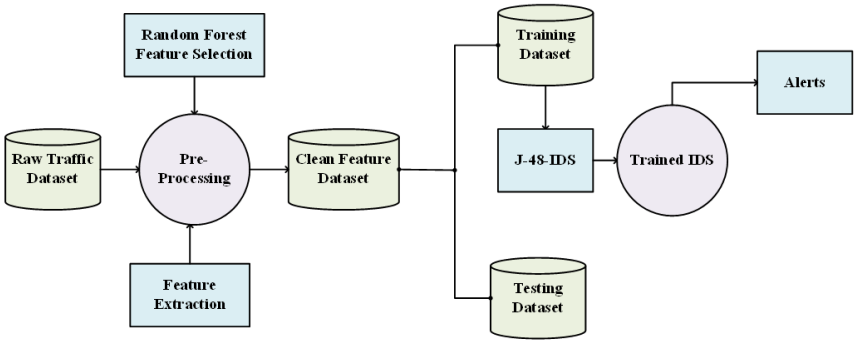

Figure 3 System Architecture of CICIDS 2017 Dataset

Figure 3 shows the System Architecture of the CICIDS 2017 Dataset contains a comprehensive system traffic reproduction agenda used to produce labelled datasets for IDS training. It contains multiple types of machinery, such as data collection, traffic cohort, and attack recreation (Thirumaran et al., 2024). The construction participates real-world traffic patterns and cyberattack situations to safeguard the dataset echoes realistic environments. It includes normal traffic alongside numerous types of attacks (e.g., DDoS, SQL injection, botnets) across different protocols. The dataset is organized to provision IDS model evaluation, providing topographies such as packet-level data and flow-level material for accurate intrusion detection.

5.2. FUTURE NEEDS IN DATASET DEVELOPMENT AND STANDARDIZATION

The future development and regulation of datasets for LSTM-based Intrusion Detection Systems (IDSS) in cloud computing surroundings face numerous insistent needs (Kim et al., 2024). One key prerequisite is the presence of more assorted attack circumstances. As cyber threats incessantly evolve, datasets must capture emergent attack practices such as innovative insistent threats (APTs), ransomware, and insider threats. Future datasets would also include a broader range of cloud-specific environments, accounting for differences in network conformations, multi-cloud buildings, and containerized requests. This assortment will help LSTM representations simplify better to various real-world scenarios. There is a need for improved labelling and annotation procedures. As physical classification is resource-intensive, future datasets should explore automated or semi-automated classification methods using progressive anomaly detection and danger intellect systems (Segun-Falade et al., 2024). This would improve the quality and accuracy of labels, dropping the balance of errors and irregularities in data. Adjustment of datasets is another critical need. A united outline for dataset construction, classification agreements, and attack organizations would endorse constancy and comparability across dissimilar research studies. Such calibration would allow for better benchmarking and association among researchers, simplifying the expansion of more effective and scalable IDSS models. There is an increasing need for real-time data cohort and unceasing dataset information to safeguard models and stay relevant in noticing the latest intimidations in self-motivated cloud surroundings.

6. APPLICATIONS OF LSTM-BASED IDS IN CLOUD ENVIRONMENTS

LSTM-based Intrusion Detection Systems (IDS) have imperative requirements in cloud surrounds due to their competence to imprisonment long-term requirements and temporal decorations in network traffic, producing them extremely actual for noticing multifaceted and growing cyberattacks. One of the principal submissions is in real-time difference detection, where LSTM models can unceasingly display cloud systems for uncommon patterns indicative of potential intrusions, such as DDoS occurrences or unauthorized access efforts. These models are predominantly valued in cloud surroundings, where the self-motivated and disseminated environment of the organization varieties it difficult for outmoded IDS to continue usefulness. LSTM-based IDSS can also be used in multi-tenant cloud surroundings, where manifold users share possessions, and dividing hateful activity becomes stimulating (Jim et al., 2024). By examining the chronological dependencies amongst events across different virtual machineries and ampules, LSTM replicas can detect doubtful decorations that may designate cross-tenant bouts, such as side-channel bouts or reserve appropriating. The key presentation is in prognostic threat detection, where LSTM replicas can forecast probable future attacks created on antique data. This positive method allows cloud administrators to take precautionary actions beforehand a bout fully happens. Additionally, these systems can be utilized for automated response systems, where LSTM models trigger predefined countermeasures in real-time to mitigate the effects of perceived interruptions, ensuring cloud safety and minimalizing injury. This competence improves both the competence and scalability of cloud-based IDS.

Figure 4

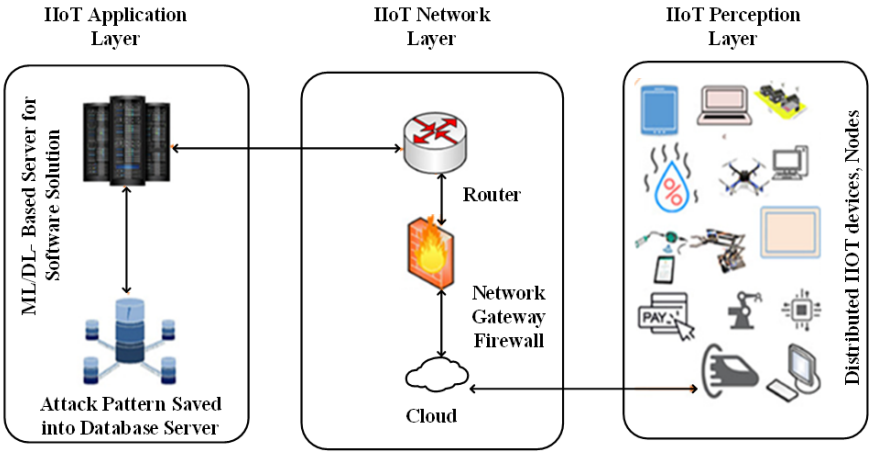

Figure 4 Intrusion Detection Systems (Ids)

Figure 4 illustrates the IDS is intended to display network traffic and organization activities to detect probable security openings or wicked happenings. The classification construction typically consists of several key components: sensors to capture data, an analyzer to process and assess the data for doubtful designs, and a forewarning device to notify supervisors about noticed pressures. IDS can be signature-based, classifying recognized threats by matching patterns, or anomaly-based, detecting deviations from normal behaviour. In contemporary applications, ML techniques like LSTM are often combined to improve the uncovering of composite, growing attacks in real-time, ornamental arrangement security.

6.1. REAL-TIME INTRUSION DETECTION IN IAAS, PAAS, AND SAAS MODELS

Real-time intrusion detection in cloud computing environments, predominantly within Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models, is important for preserving refuge and shielding in the incongruity of surfacing cyber pressures (Yang et al., 2024). In IaaS, where users are given that with virtualized manipulative properties, LSTM-based Intrusion Detection Systems (IDSS) can incessantly observe network traffic, and virtual machine (VM) activity, and reserve usage designs to notice irregularities indicative of attacks such as DDoS or unauthorized access attempts. Since IaaS atmospheres are highly dynamic, LSTM models' capability to learn time-based dependences makes them well-suited to identify long-term attack behaviours that might progress over time. For PaaS, which offers a platform for growing and managing submissions, LSTM-based IDSS can be utilized to detect malicious activity within the requests themselves (Et-Taibi et al., 2024). By examining API calls, provision communications, and data flow, the LSTM representations can catalogue unusual patterns or unofficial API admissions that might designate mistreatment of predispositions in the platform. Real-time detection in PaaS surroundings helps defend against attacks such as SQL inoculations, cross-site scripting (XSS), and privilege escalation. In SaaS environments, where users access software applications over the cloud, LSTM models can screen user behaviour, login patterns, and submission usage to detect signs of account compromise or data exfiltration. By examining chronological trends, LSTM-based systems can accurately differentiate between normal user actions and potential security breaches, providing real-time alerts and enabling prompt remediation. These capabilities across IaaS, PaaS, and SaaS models ensure inclusive refuge attention in cloud environments.

6.2. INTEGRATION WITH CLOUD MONITORING AND MANAGEMENT TOOLS

Integrating LSTM-based Intrusion Detection Systems (IDSS) with cloud nursing and organization tools is a key approach for ornamental real-time safety in cloud surroundings. Cloud monitoring tools, such as Amazon CloudWatch, Azure Monitor, and Google Cloud Operations Suite, deliver empathies into system performance, network traffic, and resource utilization. By combining these tools with LSTM-based IDSS, commissioners can create a unified security and watching infrastructure that not only detects disturbances but also provides context on system health and presentation

metrics (Anandharaj et al., 2024). LSTM models can be combined into these monitoring platforms to analyze continuous streams of data, such as CPU utilization, memory usage, and network traffic, enabling the discovery of subtle attack patterns that may not be visible through traditional monitoring tools. The unusual spikes in traffic or CPU usage that coincide with detected anomalies could suggest a DDoS attack or a botnet infection, triggering automated alerts or response actions. Cloud management tools like AWS Security Hub or Azure Security Center can be utilized to streamline incident organization by incorporating the insights from LSTM-based IDSS into broader security workflows. These stages allow for the automation of security answers, such as separating affected possessions or obstructive malicious IP addresses. This incorporation guarantees that LSTM-based arrangements not only detect intrusions but also provide criminal understandings that help in extenuating threats, cultivating an overall cloud sanctuary posture.

6.3. THREAT DETECTION IN MULTI-TENANT AND VIRTUALIZED ENVIRONMENTS

Threat detection in multi-tenant and virtualized cloud surroundings offers unique encounters due to the collective nature of possessions and the compound exchanges between different tenants. In such atmospheres, where several users or establishments share the same physical infrastructure, malicious activity by one tenant can easily impact others, making it difficult to isolate and detect threats. LSTM-based Intrusion Detection Systems (IDSS) are particularly suited for addressing these challenges due to their ability to capture temporal patterns and dependencies in network traffic, resource usage, and system logs over time. In multi-tenant environments, LSTM models can monitor interactions between virtual machines (VMs), containers, and applications to detect abnormal patterns of behaviour, such as cross-tenant attacks or resource hijacking. The infrequent spikes in CPU usage or complex traffic from one VM could indicate a denial-of-service attack or a compromised VM attempting to exploit resources from neighbouring tenants. LSTM-based replicas excel in identifying these patterns by examining time-series data and identifying deviations that may not be detectable through traditional methods. In virtualized surroundings, LSTM models can track hypervisor activity and intra-VM messages, detecting bouts that span across cybernetic machinery or involve malicious behaviour targeting hypervisor vulnerabilities. By learning long-term dependencies and interdependencies within the virtualized substructure, LSTM-based IDSS can provide more accurate and early detection of complex, stealthy occurrences that often go unnoticed in highly dynamic and shared surroundings.

6.4. ENHANCING CLOUD SECURITY POSTURE WITH AI-BASED IDS

Enhancing cloud security posture with AI-based Intrusion Detection Systems (IDS), such as LSTM-based models, is a dangerous method to preserve cloud situations against evolving cyber terrorizations. Traditional IDS may scrap to detect erudite attacks due to their reliance on predefined rules or signature-based methods. In contrast, AI-based IDS, particularly those leveraging LSTM networks, can inevitably learn complex decorations in network traffic, organization logs, and user behaviour, making them highly effective at identifying both known and unknown pressures in vigorous cloud environments (Dhruvitkumar et al., 2024). LSTM models improve cloud security by investigating time-series data, which is decisive in detecting unconventional persistent threats (APTs), DDoS attacks, and insider threats that evolve. By arresting temporal addictions in the data, LSTM networks can detect subtle, long-term attack shapes that traditional organizations might miss. These models also adapt to changing cloud organizations, guaranteeing robust safekeeping even as cloud resources are scaled or reconfigured. AI-based IDS can improve the mechanization and efficiency of incident response (Mamidi et al., 2024). With real-time detection capabilities, these arrangements can trigger immediate actions, such as separating exaggerated virtual machines or blocking malicious IPs, reducing response time and minimizing potential impairment. Integrating AI-based IDS into cloud environments strengthens the overall sanctuary carriage of a proactive defence mechanism that improves pliability to developing intimidations and susceptibilities.

7. CHALLENGES AND LIMITATIONS OF LSTM-BASED IDSS

LSTM -LSTM-based intrusion Detection Systems (IDS) have shown significant potential in detecting complex and sequential patterns of cyberattacks in cloud computing environments. However, their implementation presents several challenges and limitations. One major challenge is the high computational cost and memory requirements of LSTM models, which can hinder real-time intrusion detection in large-scale cloud systems. Training these models demands substantial processing power and large labelled datasets, which are often scarce or imbalanced in cybersecurity contexts. LSTM models are sensitive to hyperparameter settings, requiring extensive tuning to achieve optimal performance,

which can be time-consuming and resource-intensive. Another limitation is the lack of interpretability; LSTM operates as a "black box," making it difficult for security analysts to understand how decisions are made, which complicates trust and auditing. Furthermore, while LSTM excels at temporal pattern recognition, it may underperform when dealing with non-sequential or sparse data, which is common in network traffic. Scalability and deployment in dynamic cloud environments also pose issues, as cloud infrastructure and attack patterns constantly evolve. Lastly, adversarial attacks targeting AI models can potentially manipulate LSTM predictions, reducing detection accuracy. These challenges highlight the need for hybrid approaches and continuous model adaptation to ensure robust and effective cloud-based IDS. Dash et al., (2025) Proposed an optimized LSTM model, using Particle Swarm Optimization (PSO) and JAYA methods, to enhance anomaly detection in network traffic and reduce false alarm rates in IDS. To evaluate the efficacy of the proposed model, several indicators of performance like Accuracy, Precision, Recall, F-score, True Positive Rate (TPR), False Positive Rate (FPR), and Receiver Operating Characteristic curve (ROC) have been chosen. A comparative analysis of PSO-LSTMIDS, JAYA-LSTMIDS, and SSA-LSTMIDS is conducted.

7.1. SCALABILITY AND REAL-TIME PERFORMANCE IN LARGE CLOUD SYSTEMS

Scalability and real-time performance are critical requirements for Intrusion Detection Systems (IDS) in large cloud computing environments. As cloud infrastructures grow, they handle massive volumes of dynamic data generated by numerous users, applications, and virtual machines. An effective IDS must scale seamlessly to monitor and analyze this data without compromising performance. Traditional IDS often struggle to meet these demands due to limited processing capabilities and static rule-based detection. Real-time performance is equally important, as delays in classifying and responding to threats can lead to significant data breaches or service disruptions. In large cloud systems, IDS must process data streams with minimal latency while maintaining high detection accuracy. Achieving this requires optimized algorithms, distributed processing, and resource-efficient models capable of adapting to workload changes. Advanced techniques like parallel computing, edge computing, and AI-driven models, such as LSTM and ensemble learning, are increasingly employed to ensure both scalability and real-time responsiveness in securing cloud environments.

Rajesh et al. (2025) explored the challenges of managing multi-cloud environments, like data fragmentation, communication delays between clouds, and security issues. Their study highlights how technologies like microservices, container orchestration, and serverless computing can help ensure systems stay available and recover quickly from failures. They also focus on important factors such as meeting compliance requirements, reducing costs, and ensuring different cloud platforms work smoothly together. Akram et al., (2025) Cloud platforms provide the necessary scalability and computational power to support machine learning models, facilitating seamless data ingestion, processing, and deployment. Advances in distributed computing, edge AI, and serverless architectures have further optimized resource utilization and reduced latency. This paper explores the architecture of real-time AI systems, the role of cloud-based machine learning, and strategies for optimizing big data processing. By examining state-of-the-art techniques and emerging trends, this study highlights the potential of AI-driven cloud computing in enabling faster and more intelligent data-driven insights.

7.2. INTERPRETABILITY AND EXPLAINABILITY OF LSTM DECISIONS

Interpretability and explainability are significant challenges when using LSTM networks for Intrusion Detection Systems (IDS), especially in critical cloud computing environments. LSTM models, while powerful in capturing temporal dependencies and complex attack patterns, function as "black-box" systems. This means their internal decision-making processes are not easily understandable by humans, including security analysts and system administrators. Lack of interpretability makes it difficult to justify or validate why a particular network behaviour was classified as malicious or benign, which is crucial for trust, auditing, and compliance in cybersecurity. Furthermore, when false positives or false negatives occur, analyzing the model's reasoning is often impractical, limiting opportunities for improvement or retraining. This opacity also poses challenges in regulatory environments where explainable AI is increasingly required. Addressing these limitations involves integrating model-agnostic explainability tools, such as SHAP or LIME, or combining LSTM with more interpretable models to enhance transparency without compromising detection performance.

7.3. ADVERSARIAL ATTACKS AGAINST LSTM-BASED MODELS

Adversarial attacks pose a significant threat to LSTM-based models used in Intrusion Detection Systems (IDS). These attacks involve subtly modifying input data to mislead the model into making incorrect predictions classifying malicious traffic as benign or vice versa. LSTM models, despite their strength in learning sequential data patterns, are vulnerable to such attacks because they often rely on learned statistical relationships rather than semantic understanding. Attackers can exploit this vulnerability by crafting network traffic patterns that mimic normal behaviour but carry malicious intent. These carefully constructed inputs can bypass detection, leading to data breaches or service disruptions. The black-box nature of LSTM further complicates identifying and defending against such threats, as it's difficult to trace how adversarial inputs affect decision-making. To mitigate these risks, researchers are exploring adversarial training, robust model architectures, and anomaly detection layers that can identify suspicious deviations from expected input patterns, enhancing the resilience of LSTM-based IDS. Wang et al. (2025) tackled the rising threat of ransomware in cybersecurity by introducing a new deep-learning model called LSTM-EDadver. This model combines Generative Adversarial Networks (GANs) and Carlini and Wagner (CW) attacks to boost malware detection accuracy. Tested on a dataset containing 1,328 ransomware samples from 32 different families and 519 normal files, LSTM-EDadver achieved an impressive 96.59% accuracy. This outperforms traditional models like RNN, LSTM, and GCU, which scored between 90% and 94.5%. Additionally, it significantly improved the F1-score by 2.5% to 6.6%, showing better reliability in detecting ransomware compared to earlier methods without adversarial training.

7.4. DATA PRIVACY AND ETHICAL CONSIDERATIONS IN IDS DEVELOPMENT

Data privacy and ethical considerations are critical in the development of Intrusion Detection Systems (IDS), especially in cloud computing environments where vast amounts of sensitive user data are monitored. IDS often require access to detailed network traffic, user behaviour logs, and system activities to detect potential threats. However, collecting and analyzing such data can inadvertently expose private or personally identifiable information (PII), raising serious privacy concerns. Ethically, IDS developers must ensure that data collection practices comply with privacy laws and regulations such as GDPR or HIPAA. This includes implementing data anonymization, encryption, and access controls to protect user identities and prevent misuse of data. Additionally, the deployment of AI-based IDS must be transparent and fair, avoiding biased or discriminatory decision-making that could affect specific users or groups unfairly. Balancing effective threat detection with respect for user privacy and ethical standards is essential to maintaining trust, legal compliance, and responsible use of cybersecurity technologies in modern cloud environments.

8. EMERGING TRENDS AND FUTURE DIRECTIONS IN AI-BASED CLOUD SECURITY

Emerging trends in AI-based cloud security are rapidly reshaping how organizations defend against evolving cyber threats. One major trend is the integration of advanced ML and DL models for real-time threat detection and automated incident response. These models can analyze vast volumes of cloud data, identify anomalies, and respond to zero-day attacks more effectively than traditional methods. Federated learning is also gaining traction, allowing AI models to be trained across decentralized devices without sharing raw data, thus enhancing privacy. Another growing trend is the usage of explainable AI (XAI), which aims to make AI decisions more transparent and understandable, addressing concerns around accountability and trust. AI is being combined with blockchain technology to ensure secure data integrity and traceability in cloud environments. The development of lightweight AI models is enabling better security for edge and IoT devices connected to the cloud. Looking ahead, future directions include the use of self-healing security systems that automatically adapt and recover from attacks and AI-powered Security-as-a-Service (SECaaS) offerings tailored for small to mid-sized enterprises. As cyber threats grow in sophistication, the continuous evolution of AI techniques will be essential to ensure proactive, scalable, and intelligent cloud security solutions.

8.1. ADVANCES IN DEEP LEARNING FOR CYBERSECURITY

Advances in deep learning (DL) have significantly enhanced cybersecurity by enabling more effective detection of complex and previously unknown threats. Traditional signature-based methods are limited in identifying novel attacks, whereas deep learning models, especially CNNs and RNNs, excel at detecting patterns and anomalies in large volumes of data. These models can learn intricate relationships in network traffic, identify malware, and detect advanced persistent

threats (APTs) with high accuracy. Recent developments in unsupervised and semi-supervised learning techniques have allowed DL models to detect zero-day attacks and evolving threats without requiring vast labelled datasets. Techniques like reinforcement learning are being used to develop adaptive cybersecurity systems that can learn optimal defence strategies in real-time. Deep learning's ability to process and analyze data from diverse sources, such as logs, network traffic, and even system behaviour, enhances the overall security posture. Moving forward, deep learning will continue to play a pivotal role in automating threat detection and mitigation, reducing human intervention and response time in cybersecurity systems. Kandasamy et al., (2025) introduced the AEXB Model, a hybrid DL approach that combines the feature extraction capabilities of an AutoEncoder with the classification power of XGBoost. By applying this approach to the Intrusion Detection in Smart Home (IDSH) dataset, the model achieves an impressive 97.24% accuracy, demonstrating its effectiveness in identifying anomalous network behaviour indicative of MitM attacks.

8.2. FEDERATED AND DISTRIBUTED LEARNING FOR CLOUD IDS

Federated and distributed learning are emerging techniques that are transforming cloud-based Intrusion Detection Systems (IDS) by enabling collaborative, decentralized model training while preserving data privacy (Manivannan et al., 2025). In federated learning, multiple devices or edge nodes (such as IoT devices or cloud clients) collaboratively train a global model without sharing raw data. Instead, each node trains a local model and only shares the model updates (gradients) with a central server, which aggregates them to improve the global model. This method ensures that sensitive data remains on local devices, addressing privacy concerns and regulatory compliance issues, especially in environments like healthcare or finance. Distributed learning, another way, involves the training of machine learning models across multiple distributed systems or servers, which can either share data or rely on data partitioning. Both techniques are highly effective for cloud IDS because they scale well with large datasets across cloud infrastructures and IoT devices. They also allow for faster, additional efficient model training and reduce the risk of centralized data breaches. These learning approaches enable cloud IDS to adapt quickly to new attack patterns without compromising user privacy or system performance. Rampone et al., (2025) proposed a federated learning framework for near-real-time intrusion detection in IoT environments. Federated learning enables decentralized model training across multiple devices without exchanging raw data, thereby preserving privacy and reducing communication overhead. The results show that all the algorithms used maintain an excellent identification accuracy (98% for logistic R=regression, 97% for SVM, and 100% for Random Forest). This study also reports a very short training time (less than 11 s on a single machine). The previous very low application time is also confirmed (0.16 s for over 1,697,851 packets).

9. SUMMARY

This review examines the advancement of Long Short-Term Memory (LSTM)-based intrusion detection systems (IDS) specifically designed for cloud computing environments. It emphasizes LSTM's strength in modelling temporal relationships, which is crucial for identifying complex and evolving cyber threats within the dynamic nature of cloud infrastructures. The study analyzes different LSTM architectures, datasets, and performance metrics used in recent works, highlighting progress in improving detection accuracy and minimizing false alarms. Additionally, it addresses key challenges such as handling imbalanced data and the high computational cost of LSTM models. The review suggests future research should focus on enhancing the scalability of these systems, enabling real-time threat detection, and combining LSTM with other artificial intelligence methods to build more robust and efficient cloud security solutions. This ongoing development is vital to meet the increasing security demands of cloud-based services.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Olaoye, G., 2025. AI-Driven Intrusion Detection and Prevention Systems (IDPS) for Cloud Security. Available at SSRN 5129525.

Thiagarajan, G. and Mahalingam, S., 2025. Advanced Deep Learning Techniques for Anomaly Detection in Cloud Computing Traffic: Methods and Applications. Available at SSRN 5082090.

Aljuaid, W.A.H. and Alshamrani, S.S., 2024. A deep learning approach for intrusion detection systems in cloud computing environments. Applied Sciences, 14(13), p.5381.

Balasubramanian, P., Nazari, S., Kholgh, D.K., Mahmoodi, A., Seby, J. and Kostakos, P., 2025. A cognitive platform for collecting cyber threat intelligence and real-time detection using cloud computing. Decision Analytics Journal, 14, p.100545.

Jim, M.M.I., 2024. Cloud Security Posture Management Automating Risk Identification and Response in Cloud Infrastructures. Academic Journal on Science, Technology, Engineering & Mathematics Education, 4(3), pp.10-69593.

Wang, Y., Zhu, M., Yuan, J., Wang, G. and Zhou, H., 2024. The intelligent prediction and assessment of financial information risk in the cloud computing model. arXiv preprint arXiv:2404.09322.

Chauke, K.O., Muchenje, T. and Makondo, N., Enhancing Network Security in Multi-Cloud Environments through Adaptive Threat Detection.

Bolla, R.L., Jenie, R.P. and Bobba, J., 2025. The Securing Financial Cloud Services: A Novel Approach Using Identity-Chain Technology and Cluster Evaluation: Financial Cloud Services Using Identity-Chain Technology. International Journal of Digital Innovation and Discoveries, 1(01), pp.22-30.

Al-Bayati, B., Continuous User Verification in Cloud Storage Services based on Deep Learning.

Attou, H., Guezzaz, A., Benkirane, S. and Azrour, M., Cloud Security Enhancement Through RBFNN and AdaBoost-Based Model.

Düzgün, B., Çayır, A., Ünal, U. and Dağ, H., 2024. Network intrusion detection system by learning jointly from tabular and text-based features. Expert Systems, 41(4), p.e13518.

Zhao, F., Li, H., Niu, K., Shi, J. and Song, R., 2024. Application of deep learning-based intrusion detection system (IDS) in network anomaly traffic detection. Applied and Computational Engineering, 86, pp.231-237.

Alashhab, A.A., Zahid, M.S., Isyaku, B., Elnour, A.A., Nagmeldin, W., Abdelmaboud, A., Abdullah, T.A.A. and Maiwada, U.D., 2024. Enhancing DDoS attackdetection and mitigation in SDN using anensembleonlinemachinelearningmodel. IEEE Access, 12, pp.51630-51649.

Khan, N., Ahmad, K., Tamimi, A.A., Alani, M.M., Bermak, A. and Khalil, I., 2024. Explainable AI-based Intrusion Detection System for Industry 5.0: An Overview of the Literature, associated Challenges, the Existing Solutions, and Potential Research Directions. arXiv preprint arXiv:2408.03335.

Gujar, S.S., 2024, October. AI-Enhanced Intrusion Detection Systems for Strengthening Critical Infrastructure Security. In 2024 Global Conference on Communications and Information Technologies (GCCIT) (pp. 1-7). IEEE.

Dash, N., Chakravarty, S., Rath, A.K., Giri, N.C., AboRas, K.M. and Gowtham, N., 2025. An optimized LSTM-based deep learning model for anomaly network intrusion detection. Scientific Reports, 15(1), p.1554.

Rajesh, S.C. and Goel, L., 2025. Architecting Distributed Systems for Real-Time Data Processing in Multi-Cloud Environments.

Akram, F. and Sani, M., 2025. Real-Time AI Systems: Leveraging Cloud Computing and Machine Learning for Big Data Processing.

Wang, P., Lin, H.C., Chen, J.H., Lin, W.H. and Li, H.C., 2025. Improving Cyber Defense Against Ransomware: A Generative Adversarial Networks-Based Adversarial Training Approach for Long Short-Term Memory Network Classifier. Electronics, 14(4), p.810.

Kandasamy, V. and Roseline, A.A., 2025. Harnessing advanced hybrid deep learning model for real-time detection and prevention of man-in-the-middle cyber-attacks. Scientific Reports, 15(1), p.1697.

Rampone, G., Ivaniv, T. and Rampone, S., 2025. A Hybrid Federated Learning Framework for Privacy-Preserving Near-Real-Time Intrusion Detection in IoT Environments. Electronics, 14(7), p.1430.

Manivannan, R. and Senthilkumar, S., 2025. Intrusion detection system for network security using novel adaptive recurrent neural network-based fox optimizer concept. International Journal of Computational Intelligence Systems, 18(1), p.37.

Das, S., Tariq, A., Santos, T., Kantareddy, S.S. and Banerjee, I., 2023. Recurrent Neural Networks (RNNs): architectures, training tricks, and introduction to influential research. Machine learning for Brain disorders, pp.117-138.

Ahmed, S.A., Khalifa, E.H., Nawaz, M., Abdalla, F.A. and Mahmoud, A.F., 2025. Enhancing Cloud Data Center Security through Deep Learning: A Comparative Analysis of RNN, CNN, and LSTM Models for Anomaly and Intrusion Detection. Engineering, Technology & Applied Science Research, 15(1), pp.20071-20076.

Zi, Y., 2024. Time-Series Load Prediction for Cloud Resource Allocation Using Recurrent Neural Networks. Journal of Computer Technology and Software, 3(7).

Scientific, L.L., 2025. Hybrid Deep Learning Framework for Intrusion Detection: Integrating Cnn, Lstm, And Attention Mechanisms to Enhance Cybersecurity. Journal of Theoretical and Applied Information Technology, 103(1).

Sayegh, H.R., Dong, W. and Al-madani, A.M., 2024. Enhanced intrusion detection with LSTM-Based model, feature selection, and SMOTE for imbalanced data. Applied Sciences, 14(2), p.479.

Liu, Y. and Dai, Y., 2024. Deep Learning in Cybersecurity: A Hybrid BERT–LSTM Network for SQL Injection Attack Detection. IET Information Security, 2024(1), p.5565950.

Udurume, M., Shakhov, V. and Koo, I., 2024. Comparative Analysis of Deep Convolutional Neural Network Bidirectional Long Short-Term Memory and Machine Learning Methods in Intrusion Detection Systems. Applied Sciences, 14(16), p.6967.

Lee, M.C., Lin, J.C. and Katsikas, S., 2024. Exploring the effects of RNNs and deep learning frameworks on real-time, lightweight, adaptive time series anomaly detection. Concurrency and Computation: Practice and Experience, 36(28), p. e8288.

Mungoli, N., 2023. Scalable, distributed AI frameworks: leveraging cloud computing for enhanced deep learning performance and efficiency. arXiv preprint arXiv:2304.13738.

Arjunan, T., 2024. Real-time detection of network traffic anomalies in big data environments using deep learning models. International Journal for Research in Applied Science and Engineering Technology, 12(9), pp.10-22214.

Saha, S., Haque, A. and Sidebottom, G., 2024. Overcoming Data Limitations in Internet Traffic Forecasting: LSTM Models with Transfer Learning and Wavelet Augmentation. arXiv preprint arXiv:2409.13181.

Rajashekaran, K., Kazmi, R. and Jain, R.,2024. Machine Learning-Enhanced IDS: RFE-LSTM-Based Model for Cloud Security.

Aljuaid, W.A.H. and Alshamrani, S.S., 2024. A deep learning approach for intrusion detection systems in cloud computing environments. Applied Sciences, 14(13), p.5381.

Chowdhury, R., Inshi, S., Ould-Slimane, H., Talhi, C. and Mourad, A., 2025. Dynamic Real-Time Framework for Abnormal Detection of IMS Core in Kubernetes Cloud. Computer Networks and Communications, pp.147-166.

Hariharan, S., Jerusha, Y.A., Suganeshwari, G., Ibrahim, S.S., Tupakula, U. and Varadharajan, V., 2025. A Hybrid Deep Learning Model for Network Intrusion Detection System using Seq2Seq and ConvLSTM-Subnets. IEEE Access.

Salman, A.M., Al-Nuaimi, B.T., Subhi, A.A., Alkattan, H. and Alfilh, R.H., 2025. Enhancing cybersecurity with machine learning: A hybrid approach for anomaly detection and threat prediction. Mesopotamian Journal of Cybersecurity, 5(1), pp.202- 215.

Sajid, M., Malik, K.R., Almogren, A., Malik, T.S., Khan, A.H., Tanveer, J. and Rehman, A.U., 2024. Enhancing intrusion detection: a hybrid machine and deep learning approach. Journal of Cloud Computing, 13(1), p.123.

Kamal, H. and Mashaly, M., 2025. Enhanced Hybrid Deep Learning Models-Based Anomaly Detection Method for Two-Stage Binary and Multi-Class Classification of Attacks in Intrusion Detection Systems. Algorithms, 18(2), p.69.

Gong, P., Ma, Y., Li, C., Ma, X. and Noh, S.H., 2023. Understand Data Preprocessing for Effective End-to-End Training of Deep Neural Networks. arXiv preprint arXiv:2304.08925.

Smendowski, M. and Nawrocki, P., 2024. Optimizing multi-time series forecasting for enhanced cloud resource utilization based on machine learning. Knowledge-Based Systems, 304, p.112489.

Brightwood, S. and Seraphina Brightwood, A., 2024. Data Preprocessing and Feature Engineering for Cyber Threat Detection [online]

Omer, S.Z., Hashim, F., Sali, A. and Ahmad, F.A., 2025. Binary classification of Low-Rate DoS attacks using Long Short-Term Memory Feed-Forward (LSTM-FF) Intrusion Detection System (IDS). Engineering Science and Technology, an International Journal, 66, p.102049.

Kaushik, B., Sharma, R., Dhama, K., Chadha, A. and Sharma, S., 2023. Performance evaluation of learning models for intrusion detection system using feature selection. Journal of Computer Virology and Hacking Techniques, 19(4), pp.529-548.

Tripathy, S.S. and Behera, B., 2023. Performance evaluation of machine learning algorithms for intrusion detection system. arXiv preprint arXiv:2310.00594.

M.A.M.A. Hawawreh, E. Sitnikova, N. Aboutorab, X-iiotid: A connectivityagnostic and device-agnostic intrusion data set for industrial internet of things, IEEE Internet Things J. 9 (2022) 3962–3977.

A. Makkar, T.W. Kim, A.K. Singh, J. Kang, J.H. Park, Secureiiot environment: Federated learning empowered approach for securing IIOT from data breach, IEEE Transactions on Industrial Informatics (Early Access. doi: 10.1109/TII.2022.3149902.

M.A. Hawawreh, E. Sitnikova, N. Aboutorab, Asynchronous peer-to-peer federated capability-based targeted ransomware detection model for industrial iot, IEEE Access 9 (2021) 148738–148755.

L. Thi-Thu-Huong, E. Yustos, K. Howon, Xgboost for imbalanced multiclass classification-based industrial internet of things intrusion detection systems, Sustainability 14. doi: 10.3390/su14148707.

Altunay, H.C. and Albayrak, Z., 2023. A hybrid CNN+ LSTM-based intrusion detection system for industrial IoT networks. Engineering Science and Technology, an International Journal, 38, p.101322.

Mohamed, D. and Ismael, O., 2023. Enhancement of an IoT hybrid intrusion detection system based on fog-to-cloud computing. Journal of Cloud Computing, 12(1), p.41.

Srilatha, D. and Thillaiarasu, N., 2023. Implementation of Intrusion detection and prevention with Deep Learning in Cloud Computing. Journal of Information Technology Management, 15(Special Issue), pp.1-18.

Alohali, M.A., Elsadig, M., Al-Wesabi, F.N., Al Duhayyim, M., Mustafa Hilal, A. and Motwakel, A., 2023. Enhanced Chimp optimization-based feature selection with fuzzy logic-based intrusion detection system in cloud environment. Applied Sciences, 13(4), p.2580.

Al-Ghuwairi, A.R., Sharrab, Y., Al-Fraihat, D., AlElaimat, M., Alsarhan, A. and Algarni, A., 2023. Intrusion detection in cloud computing based on time series anomalies utilizing machine learning. Journal of Cloud Computing, 12(1), p.127.

Gulia, N., Solanki, K., Dalal, S., Dhankhar, A., Dahiya, O. and Salmaan, N.U., 2023. Intrusion Detection System Using the G-ABC with Deep Neural Network in Cloud Environment. Scientific Programming, 2023(1), p.7210034.

Bakro, M., Kumar, R.R., Alabrah, A., Ashraf, Z., Ahmed, M.N., Shameem, M. and Abdelsalam, A., 2023. An improved design for a cloud intrusion detection system using hybrid features selection approach with ML classifier. IEEE Access, 11, pp.64228-64247.

Alzughaibi, S. and El Khediri, S., 2023. A cloud intrusion detection system based on DNN using backpropagation and PSO on the cse-cic-ids2018 dataset. Applied Sciences, 13(4), p.2276.

Althobaiti, T., Sanjalawe, Y. and Ramzan, N., 2023. Securing Cloud Computing from Flash Crowd Attack Using Ensemble Intrusion Detection System. Computer Systems Science & Engineering, 47(1).

Basahel, A.M., Yamin, M., Basahel, S.M. and Lydia, E.L., 2023. Enhanced coyote optimization with deep learning based cloud-intrusion detection system. Computers, Materials & Continua, 74(2), pp.4319-4336.

Bukhari, O., Agarwal, P., Koundal, D. and Zafar, S., 2023. Anomaly detection using ensemble techniques for boosting the security of intrusion detection system. Procedia Computer Science, 218, pp.1003-1013.

Hidayat, I., Ali, M.Z. and Arshad, A., 2023. Machine learning-based intrusion detection system: an experimental comparison. Journal of Computational and Cognitive Engineering, 2(2), pp.88-97.