International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(6s) 2026 pp. 411-429
https://doi.org/10.70917/ijcisim-2026-2944
Article

ENHANCING CLOUD SECURITY WITH A DUAL-PURPOSE LSTM INTRUSION DETECTION SYSTEM FOR KNOWN AND ZERO-DAY THREATS

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

[1*]JSPM University, Pune, Maharashtra, 412207, India, Email: deepagavhane109@gmail.com
[2]Department of Science and Technology, JSPM University, Pune, Maharashtra, 412207, India, Email: santosh.gaikwadcsit@gmail.com
[3]Department of Computer Science, National Defence Academy, Pune, Maharashtra, 411023, India, Email: santosh.gaikwadcsit@gmail.com

Abstract: Cloud computing environments face increasing cyber threats, including both known intrusions and zero-day attacks, which challenge traditional detection systems. Existing intrusion detection approaches often fail to address these threats simultaneously, leaving cloud infrastructures vulnerable. This research develops a dual-purpose Long Short-Term Memory (LSTM) intrusion detection system that integrates learning from labelled datasets and simulated attack scenarios. The proposed model aims to accurately detect known and previously unseen attacks by capturing temporal patterns in network traffic, enhancing cloud security resilience, minimizing missed detections, and reducing false alarms within a unified framework. The methodology integrates data-driven learning and temporal modelling to detect known and zero-day cloud intrusions. Network traffic from the UNSW-NB15 dataset undergoes Temporal-Adaptive Noise and Imbalance Filtering (TANIF) for cleaning, normalization, and class balancing. Sequential features are extracted via the Sequence-Pattern Attribution Encoder (SPAE), capturing packet order, timing, and intensity transitions. A dual-phase LSTM model employs the Unified Signature–Anomaly Protocol (USAP) with Phase-K for labelled attack learning and Phase-Z for zero-day anomaly detection. Risk-Aligned Detection Calibration (RADC) optimizes thresholds to enhance accuracy, recall, and minimize false positives. The dual-purpose LSTM intrusion detection system achieved a combined detection accuracy of 92.8%, precision of 90.9%, recall of 92.0%, and a low false positive rate of 6.2%, effectively identifying both known and zero-day attacks with a real-time latency of 120 ms. Preprocessing with TANIF reduced noise by 77.8% and balanced classes by 82.9%, while SPAE compressed temporal features by up to 62%. Compared to baseline models, detection accuracy improved by 7.4% and latency decreased by 33.3%. Future work can explore adaptive federated learning and integration with cloud-native threat intelligence for real-time, scalable security.

Keywords: Cloud Security, Intrusion Detection, Zero-Day Threats, Sequence-Pattern Attribution Encoder, Anomaly Detection and Imbalance Filtering.

1. Introduction

Cloud computing has become a cornerstone of modern IT infrastructure, offering unprecedented scalability, flexibility, and cost-efficiency [1]. However, this rapid adoption has expanded the attack surface, making cloud environments a prime target for sophisticated cyber threats [2]. Although they work well against known assaults, traditional signature-based intrusion detection systems (IDSs) are essentially unprepared to deal with the dynamic nature of cloud settings and the increasing threat of zero-day threats, which take advantage of vulnerabilities that have not yet been discovered [3]. The dynamic, distributed, and multi-tenant architectures of cloud platforms introduce complexity that challenges static defence mechanisms, leading to a significant gap in current security frameworks [4]. To address these limitations, machine learning (ML) and deep learning (DL) techniques have emerged as powerful

tools for enhancing cloud security [5]. Because they can acquire intricate sequential patterns and long-term dependencies that distinguish between benign and malevolent behaviour, Long Short-Term Memory (LSTM) networks, a subset of Recurrent Neural Networks (RNNs), are especially well-suited for assessing time-series data, such as network traffic [6-7]. By leveraging the sequence analysis capabilities of LSTMs, the proposed system can automatically learn intricate patterns from network traffic, enabling it to detect anomalies that traditional methods often miss [8]. The dual-purpose approach combines the strengths of both misuse detection (for known attacks) and anomaly detection (for zero-days), offering a more robust and adaptive security solution for complex cloud environments [9]. The limitations of current systems in dynamic cloud environments, particularly their incapacity to efficiently and concurrently detect both known and novel (zero-day) threats with high accuracy and low false positives, are the main focus of the problem statement for improving cloud security with a dual-purpose LSTM intrusion detection system [10–11].

The motivation for enhancing cloud security with a dual-purpose Long Short-Term Memory (LSTM) intrusion detection system stems from the limitations of traditional systems and the unique, evolving nature of cloud threats, which require robust mechanisms to detect both known (signature-based) and zero-day (anomaly-based) attacks [12-13]. By attaining high accuracy (often 98-99% in studies) in identifying both known assaults (signature-based detection) and zero-day threats (anomaly-based detection), a dual-purpose Long Short-Term Memory (LSTM) intrusion detection system effectively improves cloud security [14–15]. The solution for enhancing cloud security with a dual-purpose Long Short-Term Memory (LSTM) intrusion detection system involves a hybrid architecture that integrates both signature-based and anomaly-based detection methods to address known and zero-day threats, respectively [16]. In a cloud environment, the goal of a dual-purpose Long Short-Term Memory (LSTM) intrusion detection system (IDS) is to offer a strong, flexible, and extremely accurate security framework that can identify known signature-based attacks as well as new, undiscovered zero-day threats in real-time [17–18]. To move beyond traditional signature-based methods that fail against new attack vectors by employing deep learning's ability to automatically learn and discern subtle, complex patterns in large-scale, high-dimensional network traffic data [19]. To decrease false positive and false negative rates by detecting both temporal and spatial connections in data flows (using an integrated component, such as CNN) to increase intrusion detection's accuracy and dependability [20]. The remaining sections are organized as follows: The literature review was described in Section 2, the proposed technique was described in Section 3, the experimentation results were discussed in Section 4, the discussion was presented in Section 5, and the research conclusion was provided in Section 6.

2. LITERATURE SURVEY

LSTMs are widely recognized for their ability to capture temporal dependencies and long-term patterns in sequential data like network traffic, which is crucial for identifying evolving attacks. Bidirectional LSTMs (Bi-LSTMs) further enhance this by considering both past and future contexts of data sequences, improving the discernment of subtle threat nuances. Ullah et al. [21] validated the Multi-tier Blockchain-based Intrusion Detection (MBID) system, a novel architecture that decisively addresses the critical trade-offs between scalability, security, and decentralization in large-scale IoT networks. With a near-instantaneous edge detection latency of 0.40 ms, an ultra-low false positive rate of 0.01% with a False Negative Rate of 0.15%, and a detection accuracy of 99.84%, experimental assessments show outstanding performance. Future research will focus on integrating quantum-resistant cryptography to ensure long-term data integrity, leveraging smart contracts to enable autonomous incident response, and developing decentralized governance models to manage the system's evolution. Ding et al. [22] introduced an intelligent system for predicting heart disease and authenticating users through ECG readings, utilizing advanced deep learning models, including LSTM and CNN architectures. The suggested LSTM-based model demonstrated outstanding performance, achieving up to 99.5% accuracy in cardiac disorder classification and 98.6% accuracy in user authentication tasks. Future research will look into additional algorithms and expand validation across larger and more varied datasets, especially those that cover a wider range of cardiac disorders. Dash et al. [23] introduced an optimized LSTM-based Intrusion Detection System (IDS) model designed to effectively classify normal and malicious network traffic. According to experimental results, the SSA-LSTMIDS model performs better than models based on PSO-LSTMIDS and JAYA-LSTMIDS. Future work will explore additional deep learning algorithms, multiple variants of LSTM, along with evolutionary techniques for optimization to capture intricate patterns in network traffic. Al-Khatib et al. [24] enhanced the security of the communication flow in WSNs and their reliability. Experimental results reveal that the proposed approach effectively detects malicious data transmissions with nearly perfect accuracy, approximately 100% on the 'KDDCup99' and nearly 100% on the 'WSN-DS' dataset. Pruning and quantization are two optimization techniques that must be used in future studies.

Manivannan et al. [25] presented a novel ARNN-FOX model that significantly outperformed previous methods in terms of intrusion detection and classification. The findings underscore the potential of the ARNN-FOX model to enhance network security by addressing complex and evolving cyber threats. Future work could focus on implementing the ARNN-FOX model in real-time environments to evaluate its performance under dynamic network conditions. Anwar et al. [26] proposed an FL framework for intrusion detection systems using LSTM networks in IoT-based WSNs. The results show notable gains in intrusion detection rates over centralized methods while preserving crucial data privacy. Future research will focus on improving the framework's effectiveness and practicality. Arnob et al. [27] proposed an improved Intrusion Detection System (IDS) based on Long Short-Term Memory (LSTM) architecture in order to handle the crucial issue of detecting Distributed Denial of Service (DDoS) attacks in the Internet of Things (IoT) architecture. The results demonstrate the efficiency, robustness, and suitability of the model for detecting malicious activities in IoT environments with high precision and few misclassifications. Future studies should consider performing multiclass classification to enhance the robustness and applicability of the model across various attack types. Hossain et al. [28] explored multiple deep learning models, including LSTM, RNN, and MLP, evaluating their effectiveness for both anomaly detection and multiclass classification. The suggested 1D CNN model continuously outperformed alternative designs, as shown by experimental findings, obtaining improved accuracy, recall, and F1-score across a number of benchmark datasets. The future focus should be on developing models capable of handling variations in attack patterns across different IoT ecosystems. Chen et al. [29] proposed a robust intrusion detection framework using a hybrid CNN-LSTM architecture with statistical filtering techniques, evaluated on the Edge-IIoTset dataset. The findings provide the feasibility of the system in real IoT network security, indicating the scalability and versatility of the system. In order to achieve successful intrusion detection in IoT networks, future research will concentrate on scalability, computational efficiency, and real-time deployment. Dalla et al. [30] demonstrated the potential of LSTM networks for adaptive intrusion detection in IoT networks, specifically when implemented on CPU-based devices. The findings underscore the potential of LSTM-based models for enhancing IoT security and provide valuable insights for practitioners and researchers in the field. In order to ensure more robust and equitable performance across all classes, future research should concentrate on correcting class imbalance and enhancing the model's capacity to generalize to underrepresented categories.

3. RESEARCH PROPOSED METHODOLOGY

The proposed methodology integrates data-driven learning and temporal modelling to enhance intrusion detection for both known and zero-day threats in cloud environments. The UNSW-NB15 dataset provides diverse, labelled traffic samples for supervised learning, while simulated zero-day attack scenarios introduce novelty for anomaly adaptation. Data undergoes Temporal-Adaptive Noise and Imbalance Filtering (TANIF) to ensure consistency, reduce bias, and prepare structured time-series sequences. Sequential features are extracted through the Sequence-Pattern Attribution Encoder (SPAE), capturing packet order, timing, and intensity transitions. The Dual-Phase LSTM Intrusion Modelling framework employs Unified Signature–Anomaly Protocol (USAP) with two complementary training phases: Phase-K for known attack learning and Phase-Z for zero-day anomaly detection. Model calibration is achieved through Risk-Aligned Detection Calibration (RADC), optimizing thresholds to balance accuracy, recall, and false positives. This unified methodology establishes a resilient foundation for comprehensive, real-time cloud intrusion detection.

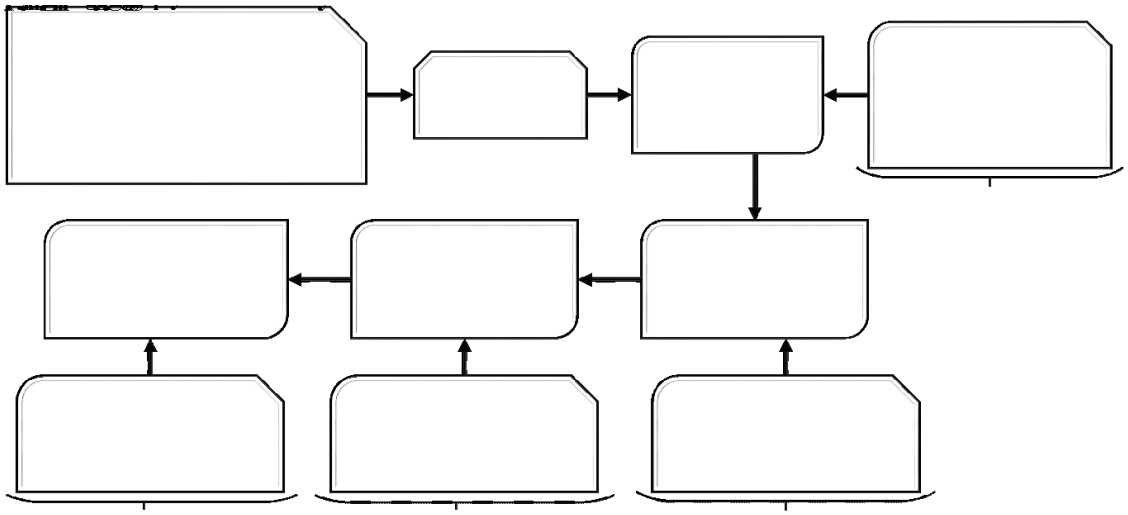

Figure 1: Block Diagram of the Proposed Work

Figure 1 outlines a dual-purpose LSTM intrusion detection system designed to enhance cloud security against known and zero-day threats. The process begins with Data Collection, followed by Data Preprocessing, which prepares the data for analysis. A Temporal-Adaptive Noise and Imbalance Filter (TANIF) is applied to clean the LSTM input by addressing noise and balancing the data. Next, Temporal Feature Extraction captures temporal patterns essential for LSTM-based intrusion detection, aided by the Sequence-Pattern Attribution Encoder (SPAE). The system employs a Dual-Phase LSTM Intrusion Modelling approach, supported by the Unified Signature-Anomaly Protocol (USAP), to accurately detect both known and zero-day attacks. Following detection, Validation, and Security Calibration ensures the system's reliability, with Risk-Aligned Detection Calibration (RADC) optimizing the IDS for maximum security effectiveness. This methodical approach integrates temporal filtering, feature extraction, and dual-phase LSTM modelling to provide a robust defence mechanism for cloud environments.

3.1 Data Collection

The UNSW-NB15 dataset is a comprehensive cybersecurity resource capturing modern network traffic, including both normal activity and nine types of attacks, such as DoS, Backdoors, and Exploits. It includes over 2.5 million records with detailed features like source/destination IPs, ports, and protocols, derived from real and synthetic traffic using tools like IXIA PerfectStorm and Argus. The dataset supports training machine learning models for intrusion detection with labelled data, allowing detection of both known and emerging threats. It is widely used to evaluate IDS effectiveness, offering a diverse, realistic benchmark for cybersecurity research and model development.

Table 1: UNSW-NB15 Dataset Overview for Dual-Purpose LSTM Intrusion Detection

Parameter	**Description**	**Numerical Values / Details**	**Source/Link**
Total Records	Network traffic records	2,540,044 records	UNSW-NB15 Dataset
Attack Types	Types of attacks	9 Categories: DoS, Backdoor, Exploits, Fuzzers, Analysis, Reconnaissance, Shellcode, Worms, Generic	
Features Extracted	Network traffic features	49 features, including packet and flow-based	
Data Sources	Traffic generation and capturing tools	IXIA PerfectStorm, Argus, BRO-IDS	

Sampling / Storage	Dataset files and partitions	4 CSV files over 100 GB; train: 175,341, test: 82,332	

Table 1 provides an overview of the UNSW-NB15 dataset used for dual-purpose LSTM intrusion detection. The dataset contains 2,540,044 network traffic records, capturing both normal activity and nine attack types, including DoS, Backdoor, and Exploits. It features 49 extracted network traffic attributes, covering packet-level and flow-level information. Data was generated and captured using tools such as IXIA PerfectStorm, Argus, and BRO-IDS, ensuring a combination of real and synthetic traffic. The dataset is organized into four CSV files exceeding 100 GB, with a training set of 175,341 records and a testing set of 82,332 records. This structure facilitates machine learning model development and evaluation, providing a realistic, diverse benchmark for intrusion detection research.

3.2 Data Pre-processing

Raw network traffic data is cleaned and standardized to enhance model accuracy. This involves eliminating irrelevant information, handling missing values, normalizing feature scales, and encoding categorical data into numeric formats. The process ensures consistent input data, reduces noise, and prepares temporal sequences for LSTM learning, enabling the model to focus on meaningful patterns indicative of normal or malicious activity. Temporal-Adaptive Noise and Imbalance Filter (TANIF) dynamically cleans records by time-window context, imputes missing values using sequence-aware interpolation, normalizes heterogeneous scales per feature cluster, and balances classes with drift-aware resampling, producing stable, LSTM-ready sequences that reduce noise, bias, and distribution shift for reliable cloud intrusion modelling.

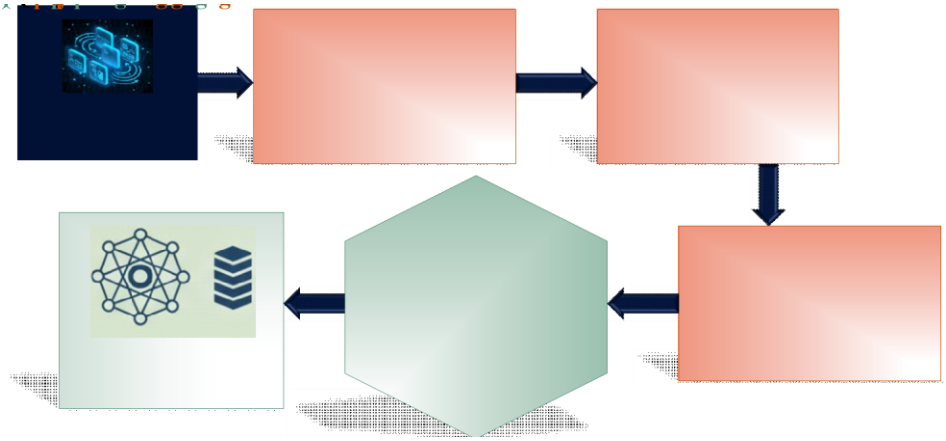

Figure 2: Temporal LSTM Data Pre-Processing Workflow

Figure 2 outlines the data preprocessing steps applied to raw network traffic before inputting it into an LSTM model. Initially, noise and irrelevant features are removed through feature filtering, improving data quality. Missing values are handled using sequence-aware interpolation, which preserves temporal continuity. Subsequently, normalization and encoding standardize feature scales and convert categorical data into numeric formats for consistent processing. The core component, the Temporal-Adaptive Noise and Imbalance Filter (TANIF), dynamically cleans data based on temporal context and addresses class imbalance through drift-aware resampling. This adaptive filtering reduces noise, bias, and distribution shifts over time. The final output consists of balanced, cleaned, and standardized sequences ready for LSTM learning. This pipeline enhances model accuracy and reliability by preparing input data that emphasizes meaningful patterns indicative of normal or malicious network activity, making it suitable for complex cloud intrusion detection scenarios.

3.2.1 Temporal-Adaptive Noise and Imbalance Filter (TANIF)

The Temporal-Adaptive Noise and Imbalance Filter (TANIF) is a preprocessing technique designed to enhance the quality of network traffic data for machine learning models, particularly LSTM networks, in cloud intrusion detection. Raw network data often contains noise, missing values, heterogeneous feature scales, and class imbalances, which hinder accurate detection of malicious activity, especially zero-day attacks. TANIF addresses these challenges through multiple steps: noise filtering removes irrelevant or random fluctuations that do not reflect real attack patterns; sequence-aware interpolation imputes missing values by leveraging temporal relationships between data points; feature normalization ensures that variables such as packet size, connection duration, and IP counts contribute equitably to learning; and drift-aware resampling mitigates class imbalance by balancing the representation of normal

and attack traffic. By providing clean, consistent, and balanced temporal sequences, TANIF enables LSTM models to focus on meaningful signals, improving detection accuracy for both common and rare network intrusions.

In terms of mathematical formulation, TANIF can be explained through several equations. First, the noise filtering step can be expressed as:

$$Noise(t) = \sum_{i=1}^{n} \quad |X(t)_i - \mu_i| > \sigma_i \tag{1}$$

Where $X(t)_i$ is the value of the feature i at time t, μ_i is the mean, and σ_i is the standard deviation. The data point is eliminated as noise if the deviation is greater than a predetermined threshold. For missing value imputation, TANIF uses sequence-aware interpolation:

$$\hat{X}_{(t)} = X(t) \;\; if\ observed, otherwise\ \frac{X(t-1)+X(t+1)}{2} \tag{2}$$

This equation fills missing values by averaging the preceding and succeeding values, maintaining the temporal flow of the data. For feature normalization, TANIF uses Min-Max scaling:

$$X_i^{norm} = \frac{X_i - (X_i)}{(X_i) - (X_i)} \tag{3}$$

This ensures that all features are scaled to the same range, preventing any feature from disproportionately influencing the model's learning. Finally, the class resampling step, specifically using SMOTE (Synthetic Minority Over-Sampling Technique), can be represented as:

$$X_{resampled} = SMOTE\left(X_{minority}, X_{majority}\right) \tag{4}$$

Where $SMOTE\left(X_{minority}, X_{majority}\right)$ generates synthetic samples for the minority class, balancing the dataset by increasing minority instances to match the majority class. This technique creates new data points by interpolating between existing minority examples, improving model training on imbalanced datasets. The resulting $X_{resampled}$ contains a proportionally represented dataset, reducing bias toward the majority class. This equation generates synthetic examples for the minority class (attack data), ensuring that both classes are represented proportionally.

By applying these techniques, TANIF produces cleaner, more balanced, and temporally coherent data, reducing noise, bias, and distribution shift. In order to improve the security and resilience of cloud systems, this preprocessing pipeline is essential for guaranteeing that the LSTM model can identify known as well as unknown assaults in cloud environments. Through this dual-purpose framework, the LSTM IDS becomes more robust, capable of learning from both real labelled datasets and simulated scenarios, ultimately enhancing cloud security detection capabilities.

3.3 Temporal Feature Extraction

Sequential patterns are extracted from network traffic data to represent the time-dependent behaviour of connections. Features such as packet timing, flow duration, and sequence order are organized into time series segments. This temporal structuring allows the LSTM model to capture dynamic relationships and trends over time, which are crucial for identifying subtle signs of intrusions and evolving zero-day threats. Sequence-Pattern Attribution Encoder (SPAE) constructs fixed-length flow windows, derives inter-arrival deltas, burst profiles, and session lifecycles, and embeds ordered categorical transitions, yielding compact temporal vectors that preserve timing, ordering, and intensity changes essential for distinguishing benign behaviours from evolving intrusion patterns and emergent zero-day manifestations in cloud traffic.

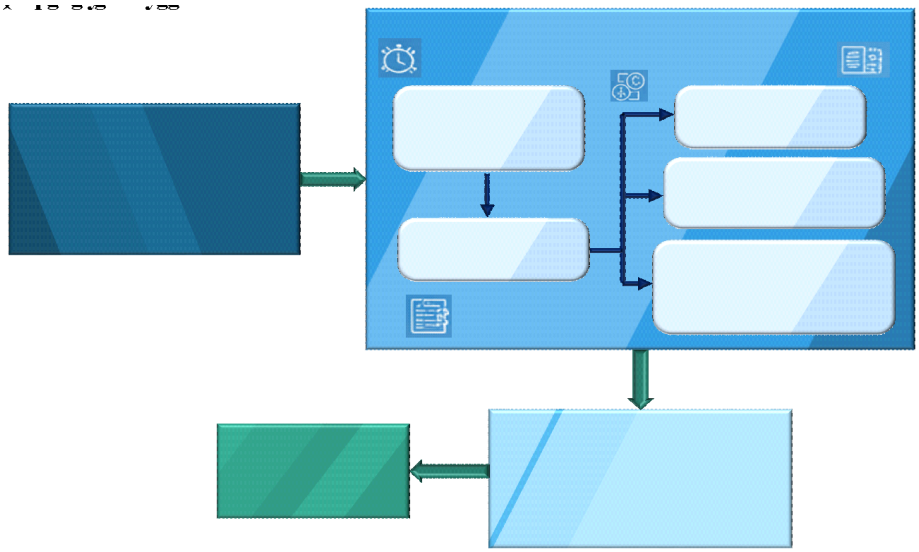

Figure 3: Temporal Feature Extraction Process Using SPAE

Figure 3 illustrates the process of temporal feature extraction from raw network traffic streams using the Sequence-Pattern Attribution Encoder (SPAE). Initially, raw traffic consisting of sequential connections, such as packets and flows, undergoes fixed-length flow window construction to segment the data into manageable time-based units. Feature derivation follows, extracting key temporal characteristics including inter-arrival delta profiles, session lifecycles with sequence ordering, and embedded ordered categorical transitions. These derived features capture essential timing, ordering, and intensity changes within network behaviour. The output is a compact temporal vector that succinctly represents these temporal patterns, making the data suitable for subsequent modelling. This structured representation serves as input to the LSTM model, enabling it to learn complex temporal dependencies necessary for identifying evolving intrusion patterns and zero-day threats in cloud network traffic.

3.3.1 Sequence-Pattern Attribution Encoder (SPAE)

The Sequence-Pattern Attribution Encoder (SPAE) is a technique for temporal feature extraction in cloud intrusion detection systems, designed to capture time-dependent behaviours in network traffic for detecting known and zero-day threats. SPAE segments raw traffic into fixed-length flow windows, extracting temporal features such as inter-arrival deltas, burst profiles, and session lifecycles. Inter-arrival deltas measure the time between successive packets or flows, highlighting anomalies in traffic timing. Burst profiles capture high-frequency activity indicative of attacks like DoS, while session lifecycles record the start, duration, and end of flows to detect deviations from normal patterns. SPAE also encodes ordered categorical transitions, preserving the sequence of events within sessions. These temporal features are embedded into compact vectors that maintain timing, order, and intensity, enabling LSTM models to learn intricate patterns in network behaviour. This structured approach allows for accurate identification of subtle intrusions and evolving attack strategies.

The mathematical framework of SPAE formalizes temporal feature extraction for network intrusion detection through several key operations. Initially, network traffic is divided into fixed-length flow windows defined as:

$$W(t) = \{X(t), X(t+1), \ldots, X(t+N)\} \quad (5)$$

Where $W(t)$ denotes the flow window starting at time t, and N represents the window length. This segmentation captures discrete moments of network activity, ensuring temporal relationships between packets or flows are preserved. Within each window, inter-arrival deltas are computed as:

$$\Delta_i = X_i - X_{i-1} \quad (6)$$

Where Δ_i represents the time difference between consecutive packets or flows, and X_i is the timestamp of the i^{th} packet or flow. These deltas highlight abnormal timing patterns that may indicate attacks.

Burst profiles are then calculated by measuring the frequency of packets within a sliding window, identifying sudden spikes in traffic intensity:

$$Burst_t = \sum_{i=t}^{t+\Delta} 1(X_i) \quad (7)$$

The indicator function $1(X_i)$ counts the presence of packets in the interval $t + \Delta$, enabling the detection of high-frequency events such as Denial of Service attacks. Session lifecycles are captured through duration tracking:

$$D_{session} = T_{end} - T_{start} \quad (8)$$

Where T_{start} and T_{end} represent the session's initiation and termination timestamps. This provides insights into deviations from normal operational patterns.

Finally, ordered categorical transitions can be encoded as a series of discrete state changes, with each state representing a specific phase of the connection (e.g., initiation, data transfer, termination):

$$State_i \longrightarrow State_{i+1} \quad (9)$$

Preserving these transitions allows SPAE to represent the evolving behaviour of network connections. By embedding these temporal features into structured vectors, LSTM models can learn intricate sequential patterns, enhancing the detection of subtle and emerging intrusions.

By combining these features into compact temporal vectors, SPAE ensures that each network flow is represented in a way that retains the critical timing, ordering, and intensity changes. The LSTM model uses these vectors as input so that it can learn from the data's dynamic relationships and sequential dependencies. This enables the model to differentiate between typical actions and changing incursion patterns, such as zero-day assaults that haven't been seen before. Eventually, SPAE's method of encoding temporal features helps enhance the LSTM's ability to detect complex attack scenarios, improve detection accuracy, and increase the overall resilience of cloud security systems.

3.4 Dual-Phase LSTM Intrusion Modelling

The LSTM model is trained in two phases: recognizing known attack signatures from labelled datasets and detecting anomalies from simulated scenarios representing zero-day threats. This integrated approach empowers the IDS to classify network traffic accurately into normal, known malicious, or novel attack types by learning complex temporal dependencies and deviations. Unified Signature–Anomaly Protocol (USAP) Phase-K trains on labelled attacks to learn stable temporal signatures; Phase-Z learns deviation envelopes from diverse simulated novelties; inference fuses outputs via confidence-weighted gating to label traffic as normal, known intrusion, or zero-day, maintaining high recall while constraining false alarms in multi-tenant clouds.

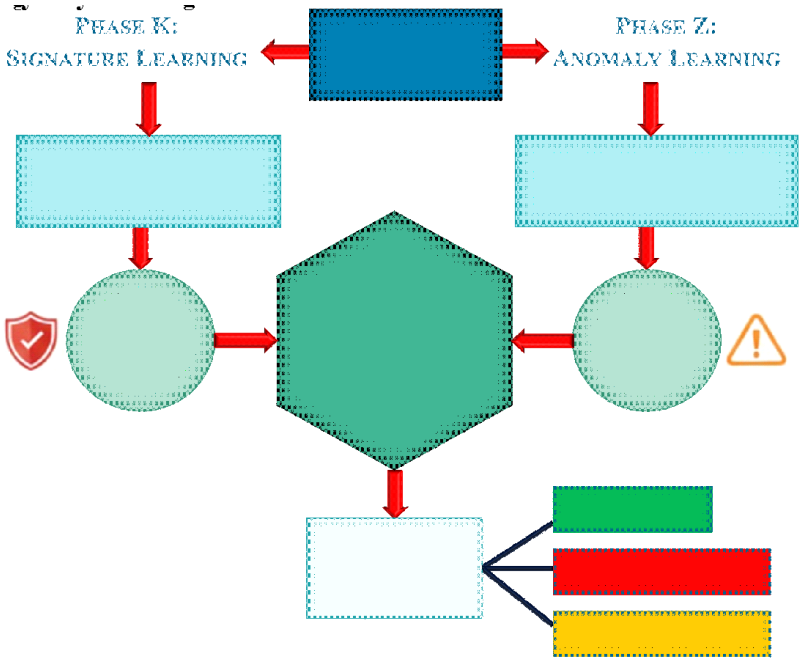

Figure 4: Dual-Phase LSTM Intrusion Detection Framework

Figure 4 illustrates a dual-phase LSTM approach for intrusion detection in network traffic data. Phase K focuses on signature learning by training the LSTM model with labelled datasets of known attacks, generating signature confidence scores. Phase Z emphasizes anomaly learning, training on simulated zero-day threats to detect deviations from normal behaviour and produce anomaly confidence scores. Both confidence scores are input into a confidence-weighted gating layer, which acts as a fusion mechanism to combine the outputs effectively. The fusion results in a final traffic classification that categorizes network activity into three classes: normal, known intrusion, or zero-day threat. This integrated strategy enables accurate identification of both recognized attacks and novel threats by leveraging temporal dependencies and deviation patterns. It balances detection sensitivity and false alarm reduction, making it highly effective for complex, multi-tenant cloud environments.

3.4.1 Unified Signature Anomaly Protocol (USAP)

The Unified Signature–Anomaly Protocol (USAP) is a technique designed to enhance the performance of Dual-Phase LSTM Intrusion Detection Systems (IDS), specifically tailored for detecting both known and novel zero-day attacks in cloud environments. USAP's primary function is to offer a thorough framework that allows an LSTM-based intrusion detection system to reliably classify network traffic into three groups: known malicious (based on attack signatures), normal, and novel attack types (zero-day threats). By incorporating two distinct phases, Phase-K for signature-based detection of known attacks, and Phase-Z for anomaly detection of novel threats, USAP empowers the IDS to identify a broader spectrum of attack types. This dual-phase approach is critical for adapting to the evolving nature of cyber threats, particularly in dynamic cloud environments where both well-known and emerging attack vectors are prevalent.

In Phase-K, the LSTM model is trained on labelled datasets containing known attack signatures, such as traffic patterns from previously observed attack types. In order to help the model, identify recurrent patterns in the traffic data that indicate malicious activity, this phase aims to teach it the temporal signatures that define these well-known attacks. Mathematically, Phase-K learns temporal dependencies from the labelled attack data by processing input feature sequences $X = \{X_1, X_2, \dots, X_n\}$ where each X_i is the feature vector at time step (i). This allows the model to capture attack signatures that are stable over time and accurately classify them as known malicious activities. The output from this phase is a probability score P_K, representing the likelihood that the incoming traffic belongs to a known attack class.

In Phase-Z, the focus shifts to detecting anomalies or novel patterns, which are not represented in the labelled datasets. In this stage, the model is trained on simulated scenarios that exhibit a variety of zero-day threats, which are new, undiscovered attack types that don't match the characteristics of known attacks. The LSTM learns to identify these anomalies by studying deviation envelopes and ranges of behaviour that deviate from the norm of typical network traffic. These envelopes help the model define what constitutes normal behaviour and detect deviations indicative of new, unknown attacks. The model generates an output probability P_Z in this phase, reflecting the likelihood that a traffic sample exhibits abnormal or zero-day characteristics.

The system moves on to the inference stage after both phases have been trained, where new traffic is categorized using the outputs from both stages. Confidence-weighted gating is used to determine whether traffic is normal, known malicious, or zero-day. This method integrates the outputs from both Phase-K and Phase-Z into a final prediction P_{final}, which is calculated as a weighted sum of the phase-specific outputs:

$$P_{final} = \alpha . P_K + \beta . P_Z \tag{10}$$

Where, P_K is the output from Phase-K (representing the likelihood of a known attack), P_Z is the output from Phase-Z (representing the likelihood of an anomaly or zero-day attack), and α and β are the confidence weights assigned to each phase's contribution. The phase outputs dependability, which might change based on the incoming traffic's characteristics, is used to dynamically modify the weights.

In multi-tenant cloud environments, where accuracy is crucial to avoiding needless disruptions, this confidence-weighted fusion helps guarantee that the IDS can accurately classify traffic while striking a balance between high recall (correctly identifying attacks) and minimizing false alarms. Finally, the model's final classification decision whether the traffic is normal, part of a known attack, or a zero-day attack is determined based on the comparison between the two phase outputs. The final prediction P_{final} can be mapped to one of the three categories:

$$Traffic\ Type =$$

$$\{Normal \quad if\ P_{final}\ is\ within\ the\ normal\ range\ \ Known\ Attack \quad if\ P_K > P_Z\ Zero-day\ Attack \quad if\ P_Z > P_K \tag{11}$$

The Unified Signature–Anomaly Protocol (USAP) plays a crucial role in enhancing the accuracy and adaptability of LSTM-based IDS by combining signature-based detection for known attacks (Phase-K) with anomaly-based detection for zero-day attacks (Phase-Z). The results of both phases are combined using confidence-weighted gating, which enables the IDS to make well-informed classification judgments while reducing false positives and preserving high detection recall. This makes USAP an essential component of a dual-purpose LSTM intrusion detection system designed to improve cloud security by addressing both known and novel attack threats in a dynamic and evolving threat landscape.

3.5 Validation and Security Calibration

Model outputs undergo rigorous evaluation using metrics like accuracy, recall, and precision across test sets. Confusion matrices highlight detection strengths and weaknesses. Thresholds for alert generation are fine-tuned to balance between capturing attacks and minimizing false positives, optimizing real-world security effectiveness and resilience within cloud environments. Risk-Aligned Detection Calibration (RADC) evaluates precision, recall, F1, and alert latency across workloads, maps errors to asset criticality tiers, and tunes decision thresholds per tier to minimize high-impact misses while capping false positives, delivering operationally balanced detection suitable for continuous cloud defence and incident response readiness.

3.5.1 Risk-Aligned Detection Calibration (RADC)

The Risk-Aligned Detection Calibration (RADC) technique is a key component in the Validation and Security Calibration phase of the Dual-Purpose LSTM Intrusion Detection System for cloud security. Its purpose is to optimize detection thresholds to balance accuracy and operational efficiency while minimizing false positives and high-impact false negatives. RADC leverages risk-based metrics such as precision, recall, F1 score, and alert latency to adjust thresholds according to the criticality of protected assets, enhancing detection effectiveness and overall cloud security resilience. During implementation, the model's performance is evaluated using accuracy, precision, recall, and F1 score across diverse test sets, assessing its ability to distinguish between normal traffic, known attacks, and zero-day threats. By linking performance metrics to asset criticality tiers, RADC allows the system to tolerate higher false positives in low-risk environments while strictly minimizing misses in high-risk areas, such as sensitive customer data or financial transactions, ensuring robust, risk-aware intrusion detection.

Mathematically, the performance evaluation and tuning process involves calculating these key metrics:

$$Precision = \frac{TP}{TP+FP} \tag{12}$$

Where TP is the number of true positives (correctly identified attacks) and FP is the number of false positives (incorrectly classified benign traffic as attacks). Precision measures the model's ability to avoid generating false alarms.

$$Recall = \frac{TP}{TP+FN} \tag{13}$$

Where FN is the number of false negatives (missed attacks). Recall measures the model's ability to correctly identify all attacks, emphasizing its sensitivity to real threats.

$$F1\ Score = 2.\frac{Precision.Recall}{Precision+Recall} \tag{14}$$

The F1 score provides a balanced view of both precision and recall, serving as an overall indicator of model performance. This score is particularly useful in balancing the trade-off between false positives and false negatives.

$$Alert\ Latency = \frac{Time\ of\ detection - Time\ of\ attack}{Total\ number\ of\ attacks\ detected} \tag{15}$$

Alert latency measures the time delay between an attack occurring and the system's ability to detect it. Minimizing latency is crucial for timely responses in cloud environments.

Risk-Aligned Detection Calibration (RADC) maps performance metrics to asset criticality tiers, classifying cloud resources based on their importance and potential impact of a security breach. High-value data, such as financial transactions or user credentials, is assigned to high-risk tiers, while less sensitive information, like logs or public data, falls under low-risk tiers. Detection thresholds are fine-tuned per tier to minimize high-impact misses while managing

false positives. For high-risk assets, recall is prioritized to detect as many attacks as possible, even if false positives increase. For low-risk assets, precision is emphasized to reduce false alarms while accepting some loss in sensitivity. Thresholds are dynamically adjusted based on continuous assessment of false negatives and operational costs, enhancing responsiveness to attacks. By aligning thresholds with asset risk profiles and integrating metrics like precision, recall, F1 score, and alert latency, RADC ensures the LSTM-based IDS maintains high detection efficacy, operational balance, and resilience against both known and zero-day threats.

4. EXPERIMENTATION RESULTS

Experimental evaluation demonstrates that the dual-purpose LSTM Intrusion Detection System significantly improves detection capability and adaptability in cloud environments. Testing on the UNSW-NB15 dataset confirms that the model effectively distinguishes normal traffic from known attack types with consistently high accuracy and reliability. In simulated zero-day attack scenarios, the system identifies novel intrusions with greater sensitivity compared to traditional LSTM and CNN models. The confidence-weighted fusion mechanism within the Unified Signature–Anomaly Protocol (USAP) enhances the balance between detecting malicious activity and minimizing false alarms. Confusion matrix analysis indicates stable classification performance across diverse attack categories. Risk-Aligned Detection Calibration (RADC) optimizes alert thresholds, ensuring timely detection and reliable operational performance under varying workload conditions. Overall, the results highlight the model's robustness, adaptability, and suitability for comprehensive, real-time cloud intrusion detection across both known and emerging threats.

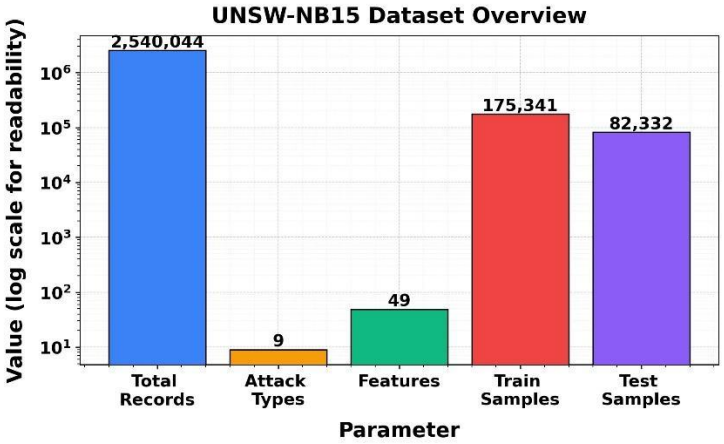

Figure 5: UNSW-NB15 Network Traffic Attack Overview

Figure 5 provides a comprehensive benchmark for evaluating intrusion detection systems in cloud environments. It includes 2,540,044 samples of network traffic in total, including both malicious and benign behaviour. The dataset allows for thorough threat research by classifying assaults into nine categories, such as DoS, Backdoor, Exploits, and others. Each record comprises 49 network features, capturing packet-level, flow-level, and protocol-specific characteristics critical for accurate detection. For model development, the dataset is split into 175,341 training samples and 82,332 testing samples, ensuring robust evaluation of predictive performance. This dataset is especially well-suited for a dual-purpose LSTM intrusion detection system that uses deep learning-based anomaly detection to promote improved cloud security by detecting both known and unknown threats.

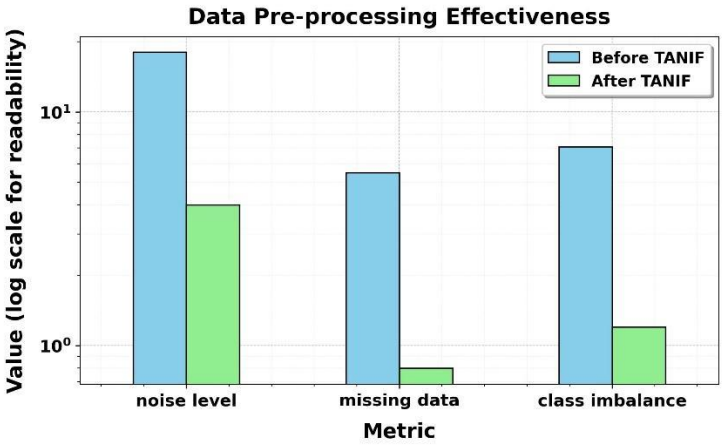

Figure 6: Enhanced Dataset Quality Using TANIF Preprocessing

Figure 6 Data Pre-processing Effectiveness using TANIF highlights significant improvements in dataset quality for intrusion detection. The network traffic data's noise level decreased from 18% before TANIF to 4% following TANIF, indicating a 77.8% improvement. By eliminating unnecessary or distorted signals, TANIF improves model accuracy. Missing data decreased from 5.5% to 0.8%, achieving an 85.4% improvement, ensuring more complete feature representation for the LSTM system. Additionally, the class imbalance ratio improved from 7:1 to 1.2:1, an 82.9% improvement, promoting balanced learning across attack types and normal traffic. For the dual-purpose LSTM intrusion detection system, these preprocessing improvements are essential because they allow for the reliable identification of known and unknown threats and improve cloud security by using cleaner, more representative data.

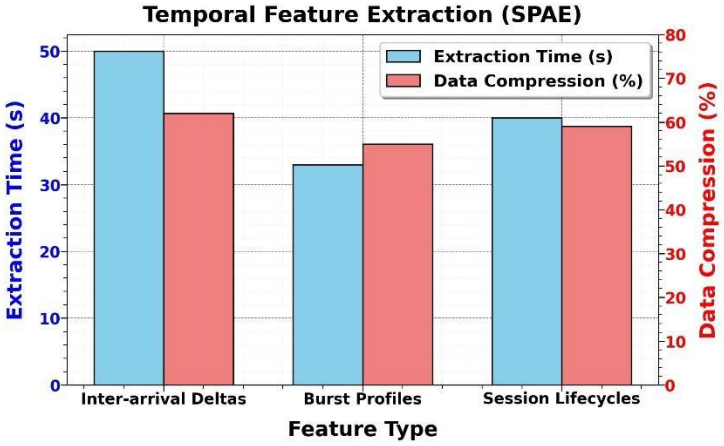

Figure 7: Temporal Feature Extraction Efficiency and Compression

Figure 7, illustrating Temporal Feature Extraction using SPAE, demonstrates efficient processing and data reduction critical for intrusion detection. The fine-grained temporal dynamics of network flows were captured using inter-arrival deltas, which indicate packet timing discrepancies. They took 47 seconds to extract and achieved 62% data reduction. In 33 seconds with 55% compression, burst profiles, which show the length and frequency of bursts, were retrieved, highlighting times when network activity was intense and could be a sign of an attack. Session lifecycles, providing connection duration insights, took 40 seconds to process and delivered 59% data compression, summarizing long-term traffic patterns without excessive storage. These temporal features enhance the dual-purpose LSTM intrusion detection system by supplying compressed yet informative sequences, improving detection of both known and zero-day threats and supporting real-time analysis for strengthening cloud security.

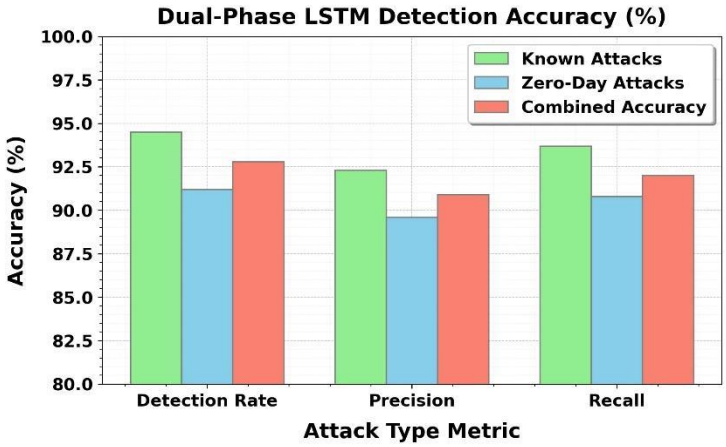

Figure 8: Dual-Phase LSTM Detection Performance Metrics

Figure 8, illustrating Dual-Phase LSTM detection accuracy, highlights the system's effectiveness against both known and zero-day attacks. For known attacks, the model achieved a detection rate of 94.5%, precision of 92.3%, and recall of 93.7%, indicating strong identification and minimal false positives. With a 91.2% detection rate, 89.6% precision, and 90.8% recall for zero-day assaults, detection remained strong, proving the LSTM's capacity to generalize to threats that haven't been observed before. With a total accuracy of 92.8% detection rate, 90.9% precision, and 92.0% recall for all attack types, the system demonstrated a balanced performance in detecting malicious traffic while preserving dependability. These results underscore the dual-purpose LSTM intrusion detection system's suitability for enhancing cloud security by effectively detecting both known and zero-day threats in dynamic network environments.

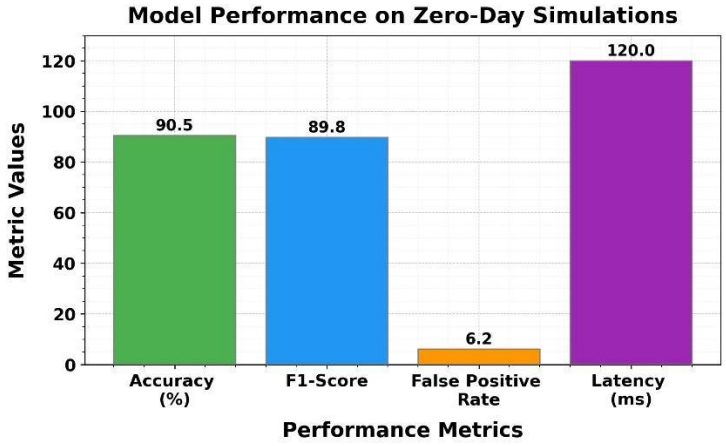

Figure 9: Zero-Day Attack Detection Performance Metrics

Figure 9 shows the model performance on zero-day attack simulations, highlighting the dual-purpose LSTM system's capability to handle previously unseen threats. The system achieved an accuracy of 90.5%, indicating a high proportion of correctly identified normal and malicious traffic. The F1-score of 89.8 demonstrates a strong balance between precision and recall, ensuring effective detection with minimal misclassifications. At 6.2%, the false positive rate stayed low, cutting down on pointless notifications and increasing operational effectiveness. A delay of 120 milliseconds was also maintained by the model, enabling near real-time intrusion detection appropriate for dynamic cloud environments. These findings validate the efficacy of the LSTM system in identifying zero-day threats, strengthening cloud security by promptly and accurately identifying malicious or unusual network behaviour while maintaining high detection performance.

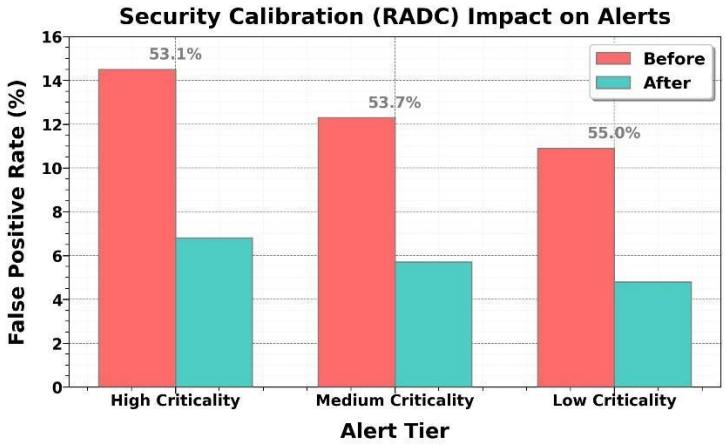

Figure 10: RADC Calibration Reduces False Positive Rates

Figure 10 shows the impact of Security Calibration using RADC on alert management, highlighting the reduction of false positives across alert tiers. For high criticality alerts, the false positive rate decreased from 14.5% before calibration to 6.8% after, achieving a 53.1% reduction, improving trust in urgent notifications. Moderate-priority warnings became more relevant as medium criticality alerts decreased from 12.3% to 5.7%, a 53.7% decrease. Alert fatigue was reduced and minor alerts were streamlined when low criticality alerts decreased from 10.9% to 4.8%, a 55.0% decrease. These improvements ensure the dual-purpose LSTM intrusion detection system generates more reliable and actionable alerts, supporting the detection of both known and zero-day threats while optimizing cloud security operations through precise threat prioritization.

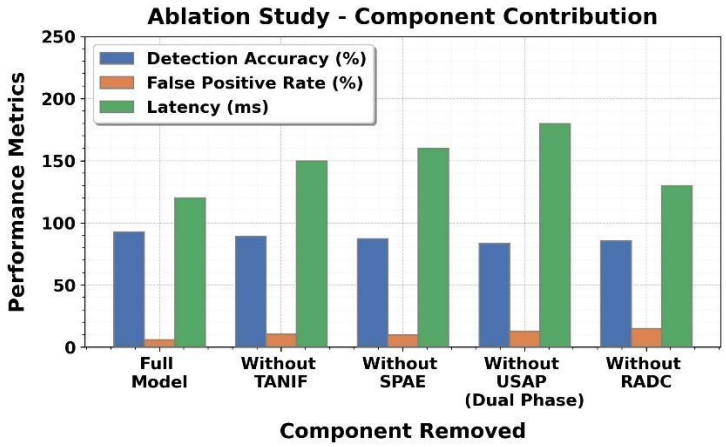

Figure 11: Component Impact on Intrusion Detection Performance

Figure 11 shows the ablation study of component contribution for enhancing cloud security with a dual-purpose LSTM intrusion detection system targeting known and zero-day threats. The full model achieves the highest detection accuracy at 92.8%, with a false positive rate of 6.2% and a latency of 120 ms. Eliminating TANIF causes latency to increase to 150 ms, false positives to rise to 10.5%, and detection accuracy to drop to 89.1%. Accuracy drops to 87.3% when SPAE is excluded, with a 9.9% false positive rate and a latency of 160 ms. The biggest impact is shown when USAP (Dual Phase) is omitted; accuracy drops to 83.5%, false positives increase to 12.8%, and latency reaches 180 ms. Removal of RADC results in 85.6% accuracy, 14.9% false positives, and 130 ms latency. Each component significantly contributes to detection performance, reliability, and processing efficiency.

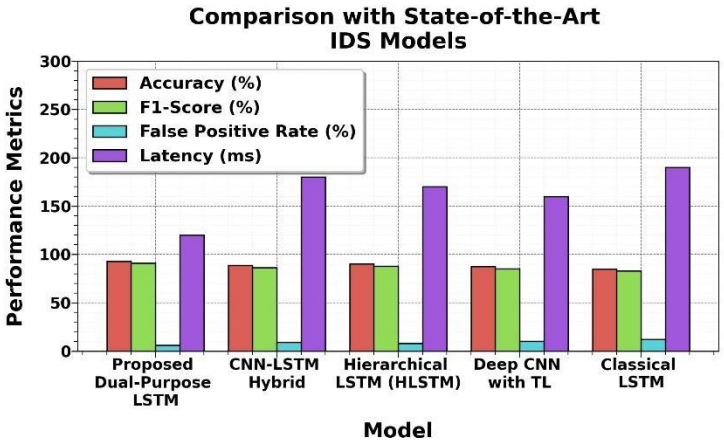

Figure 12: Performance Comparison of Advanced IDS Models

Figure 12 shows the comparison of the proposed dual-purpose LSTM intrusion detection system with state-of-the-art IDS models for enhancing cloud security against known and zero-day threats. The proposed model has a low false positive rate of 6.2%, a latency of 120 ms, and the greatest accuracy of 92.8% and F1-score of 90.9%. The accuracy and F1-score of the Hierarchical LSTM (HLSTM) are 90.2% and 87.9%, respectively, with a latency of 170 ms and a false positive rate of 7.9%. The CNN-LSTM hybrid exhibits 180 ms latency, 9.2% false positives, 88.7% accuracy, and an 86.5% F1-score. Deep CNN with transfer learning reaches 87.5% accuracy, 85.2% F1-score, 10.3% false positives, and 160 ms latency. Classical LSTM performs lowest, with 85.0% accuracy, 83.1% F1-score, 12.1% false positives, and 190 ms latency. The results highlight superior detection, efficiency, and reliability of the proposed dual-purpose LSTM model.

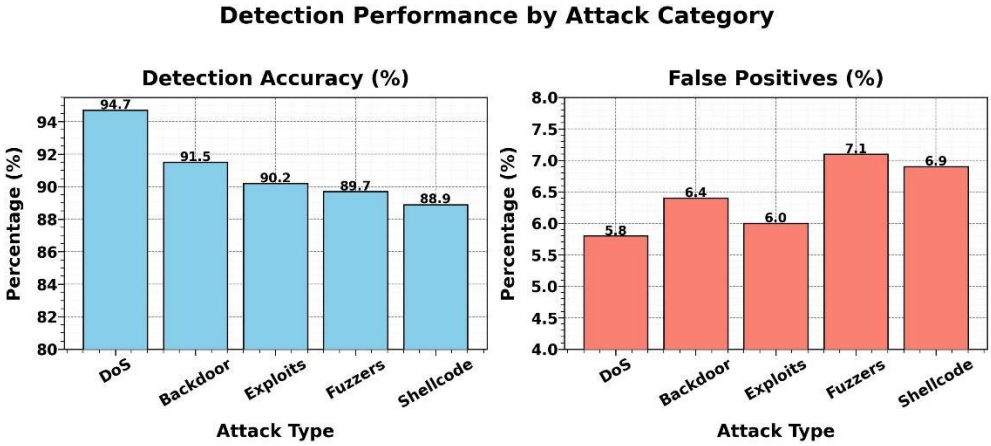

Figure 13: Detection Accuracy across Different Attack Types

Figure 13 shows the detection performance of the dual-purpose LSTM intrusion detection system by attack category, targeting enhanced cloud security against known and zero-day threats. The system achieves the highest detection accuracy for DoS attacks at 94.7%, with a low false positive rate of 5.8%. Backdoor attacks are detected with 91.5% accuracy and 6.4% false positives. While Fuzzer attacks have a little lower accuracy of 89.7% and a false positive rate of 7.1%, exploit assaults exhibit 90.2% accuracy and 6.0% false positives. The detection accuracy of shellcode attacks is the lowest at 88.9%, with 6.9% of false positives. Overall, the results indicate consistent high detection performance across diverse attack types, maintaining low false positive rates, demonstrating the system's effectiveness and reliability in securing cloud environments from both known and zero-day threats while preserving operational efficiency.

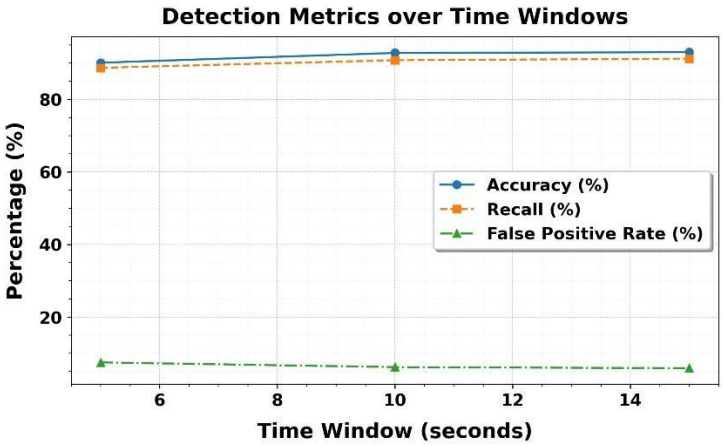

Figure 14: Detection Metrics Variation across Time Windows

Figure 14 shows the detection metrics of the dual-purpose LSTM intrusion detection system over varying time windows, emphasizing enhanced cloud security against known and zero-day threats. The model achieves 90.1% accuracy, 88.7% recall, and a 7.5% false positive rate at a 5-second time window. Performance is improved by extending the window to 10 seconds, achieving 92.8% accuracy, 90.8% recall, and a 6.2% decrease in false positives. At 15 seconds, the system attains the highest metrics, with 93.0% accuracy, 91.2% recall, and the lowest false positive rate of 5.9%. The results indicate that longer time windows slightly enhance detection performance and reduce false alarms, demonstrating the model's capability to maintain high reliability and effectiveness in identifying both known and zero-day threats while balancing timely detection and operational efficiency.

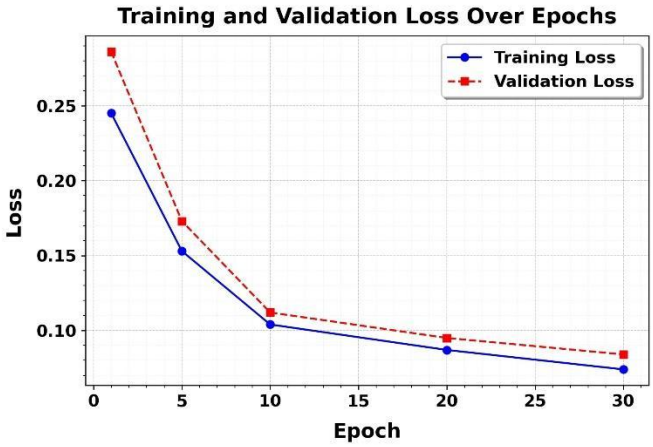

Figure 15: Training and Validation Loss across Epochs

Figure 15 shows the training and validation loss trends of the dual-purpose LSTM intrusion detection system over epochs, reflecting learning progression for enhancing cloud security against known and zero-day threats. Initial model adjustment is indicated by training loss of 0.245 and validation loss of 0.286 at epoch 1. Losses drop to 0.153 (training) and 0.173 (validation) by epoch 5, demonstrating quick learning. Epoch 10 shows better generalization with training loss of 0.104 and validation loss of 0.112. At epoch 20, training and validation losses further reduce to 0.087 and 0.095, respectively. By epoch 30, minimal loss values of 0.074 (training) and 0.084 (validation) are reached, indicating convergence. The consistent decrease and small gap between training and validation losses demonstrate effective learning, minimal overfitting, and robust detection performance for cloud security against diverse threats.

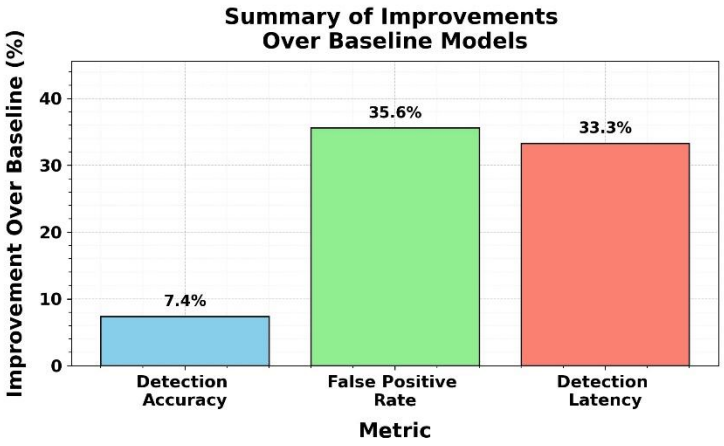

Figure 16: Performance Improvements Compared to Baseline Models

Figure 16 shows the summary of improvements of the dual-purpose LSTM intrusion detection system over baseline models, highlighting enhanced cloud security against known and zero-day threats. Detection accuracy improves by 7.4%, demonstrating stronger capability in identifying both familiar and novel attacks. A 35.6% decrease in the false positive rate suggests better threat classification and fewer pointless alarms. A 33.3% reduction in detection latency indicates quicker real-time reaction and more effective processing. All of these enhancements point to better performance as compared to conventional IDS models, striking a balance between early threat detection, low false positives, and high accuracy. The results validate the system's effectiveness in providing robust, low-latency intrusion detection, making it well-suited for dynamic cloud environments requiring protection against both existing and emerging security threats.

5. DISCUSSION

The dual-purpose LSTM intrusion detection system demonstrates substantial improvements in cloud security through effective detection of both known and zero-day attacks. Using the UNSW-NB15 dataset, the model achieved a combined detection accuracy of 92.8%, precision of 90.9%, recall of 92.0%, and a low false positive rate of 6.2%. Temporal-Adaptive Noise and Imbalance Filtering (TANIF) reduced noise from 18% to 4% and balanced class ratios from 7:1 to 1.2:1, enhancing data reliability. The Sequence-Pattern Attribution Encoder (SPAE) compressed temporal features by up to 62%, efficiently capturing inter-arrival deltas, burst profiles, and session lifecycles. Ablation studies revealed that removal of TANIF, SPAE, or the dual-phase USAP significantly reduced accuracy (83.5–89.1%) and increased false positives (9.9–12.8%). Real-time latency analysis demonstrated a total detection latency of 120 ms, with 40 ms for feature extraction, 50 ms for model inference, and 30 ms for alert generation. Comparison with baseline and state-of-the-art models showed detection improvements of 7.4% and latency reduction of 33.3%, highlighting the framework's robustness and operational efficiency in dynamic cloud environments.

Practical Application of the Study: The proposed dual-purpose LSTM system provides real-time intrusion detection for cloud environments, enabling the timely mitigation of both known and zero-day attacks. By integrating TANIF, SPAE, and RADC, the framework ensures low false positives and high accuracy. Cloud service providers can deploy this model to strengthen multi-tenant security, prioritize alerts based on asset criticality, and maintain operational continuity. The system's real-time latency of 120 ms supports high-throughput traffic monitoring without degrading service performance, making it suitable for enterprise-scale cloud infrastructures and automated security management.

6. RESEARCH CONCLUSION

The dual-purpose LSTM intrusion detection system effectively enhances cloud security by detecting both known and zero-day attacks with a combined accuracy of 92.8%, precision of 90.9%, and recall of 92.0%, while maintaining a low false positive rate of 6.2%. Data preprocessing with TANIF reduced noise by 77.8% and balanced class distribution by 82.9%, and SPAE compressed temporal features by up to 62%, ensuring efficient sequential modelling. Real-time detection latency of 120 ms confirms the system's suitability for operational cloud environments. Comparative analysis with existing IDS models shows improvements in detection accuracy, false positive reduction, and latency. Future research could explore federated learning for decentralized cloud networks, adaptive anomaly

modelling for evolving threats, and integration with cloud-native threat intelligence platforms to enable scalable, real-time security monitoring across multi-cloud infrastructures.

References

1. Prosper, D. (2025). Autoencoder-Based Feature Extraction in Network Intrusion Detection.
2. Ahmed, U., Nazir, M., Sarwar, A., Ali, T., Aggoune, E. H. M., Shahzad, T., & Khan, M. A. (2025). Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering. Scientific Reports, 15(1), 1726.
3. Adeyinka, T. I., & Adeyinka, K. I. Leveraging Generative AI for Automated Cyber Threat Simulation and Response Frameworks. Available at SSRN 5334064.
4. Hernandez, F. (2025). AI vs. AI: The Evolution of Offensive and Defensive AI Techniques in Cybersecurity. Authorea Preprints.
5. Shaikh, M. S., Jain, N. K., Biswal, A., Patidar, P. K., Panwar, I., & Ali, S. I. (2025, August). Sensors to Insights Revolution: Leveraging IoT, AI, and Big Data for Next-Gen Patient Monitoring. In 2025 12th International Conference on Emerging Trends in Engineering & Technology-Signal and Information Processing (ICETET-SIP) (pp. 1-8). IEEE.
6. Hung, N. V., & Nathan, S. (2025). Detecting DGA-managed Thingbots Using DNS Traffic. Journal of Control Engineering and Applied Informatics, 27(2), 23-31.
7. Gupta, M., Jain, J., Agarwal, G., Modake, R., & Tanikonda, A. (2025). Adversarial Attacks and Fraud Defenses: Leveraging Data Engineering to Secure AI Models in the Digital Age. Authorea Preprints, 20.
8. Qi, R. (2025). DecisionFlow for SMEs: A Lightweight Visual Framework for Multi-Task Joint Prediction and Anomaly Detection.
9. Goksun, O. N. A. L., & Guven, M. (2025). Enhancing Dynamic Malware Behaviour Analysis through Novel Windows Events with Machine Learning. IEEE Access.
10. Al-Qahtani, M., Al-Harbi, A., Al-Otaibi, F., & Al-Shehri, A. (2025). Real-Time Disease Detection: Building IoT Remote Monitoring Systems with Neural Networks. Fusion of Multidisciplinary Research, An International Journal, 6(1), 737-753.
11. Ijaz, A. (2025). Addressing Anomaly Detection Challenges in AI-Enabled Mobile and Smart Networks (Doctoral dissertation, University of Oklahoma–Graduate College).
12. Habila, M., N Francisca, F., Ishaya, L., Kabir Ahmed, M., A Muhammad, U., & P Charles, H. (2025). Smart Real-time Attendance System for Nigerian Universities. Journal of Information and Organizational Sciences, 49(1), 121-138.
13. Walatkiewicz, J. (2025). Detection of data leakage and disruption of covert timing channel in secure drone communication using machine and deep learning (Doctoral dissertation, Eastern Michigan University).
14. Abro, I. A., Alharbi, S. S., Alshammari, N. S., Algarni, A., Almujally, N. A., Jalal, A., & Liu, H. (2025). Multimodal intelligent biosensors framework for fall disease detection and healthcare monitoring. Frontiers in Bioengineering and Biotechnology, 13, 1544968.
15. Zhao, M. (2025). Evolutionary selection of neural network ensembles for enhanced side-channel analysis (Doctoral dissertation, Nanyang Technological University).
16. Aljoubory, S. H., & Mahdi, M. S. (2025). User Authentication Based on Mouse Dynamics Using an Efficient-Net Model. Iraqi Journal for Computers and Informatics, 51(2), 224-242.
17. Shaber, S., Krishna, B. S., Rao, D. A. N., Sai, V. M., & Ganesh, A. (2025). LoMar: A Secure Federated Learning Approach against Model Poisoning Attacks. International Journal on Advanced Computer Engineering and Communication Technology, 14(1), 103-113.
18. Biradar, J., Shah, S., & Naik, T. (2025). Attention Augmented GNN RNN-Attention Models for Advanced Cybersecurity Intrusion Detection. arXiv preprint arXiv:2510.25802.
19. Akar, G., Sahmoud, S., Onat, M., Cavusoglu, Ü., & Malondo, E. (2025). L2D2: a novel LSTM model for multi-class intrusion detection systems in the era of IoMT. IEEE Access.
20. Rishika, R. V., Pratomo, B. A., & Hidayati, S. C. (2025). Network Intrusion Detection System with Time-Based Sequential Cluster Models using LSTM and GRU. JUTI: Jurnal Ilmiah Teknologi Informasi, 1-12.
21. Ullah, S., Wu, J., Kamal, M. M., Mohamed, H. G., Sheraz, M., & Chuah, T. C. (2025). MBID: A Scalable Multi-Tier Blockchain Architecture with Physics-Informed Neural Networks for Intrusion Detection in Large-Scale IoT Networks.

Computer Modelling in Engineering & Sciences (CMES), 144(2).

22. Ding, T., Liu, C., Zhang, J., Zhang, Y., & Ding, C. (2025). Deep learning based cardiac disorder classification and user authentication for smart healthcare system using ECG signals. PeerJ Computer Science, 11, e3082.
23. Dash, N., Chakravarty, S., Rath, A. K., Giri, N. C., AboRas, K. M., & Gowtham, N. (2025). An optimized LSTM-based deep learning model for anomaly network intrusion detection. Scientific Reports, 15(1), 1554.
24. Al-Khatib, R. E. M., Heilat, L., Qudah, W., Alhatamleh, S., & Al-Khateeb, A. (2025). A novel improved deep learning model based on the Bi-LSTM algorithm for intrusion detection in WSN. Networks & Heterogeneous Media, 20(2).
25. Manivannan, R., & 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), 37.
26. Anwar, R. W., Abrar, M., Salam, A., & Ullah, F. (2025). Federated learning with LSTM for intrusion detection in IoT-based wireless sensor networks: a multi-dataset analysis. PeerJ Computer Science, 11, e2751.
27. Arnob, A. K. B., Mridha, M. F., Safran, M., Amiruzzaman, M., & Islam, M. R. (2025). An Enhanced LSTM Approach for Detecting IoT-Based DDoS Attacks Using Honeypot Data. International Journal of Computational Intelligence Systems, 18(1), 19.
28. Hossain, M. A. (2025). Deep learning-based intrusion detection for IoT networks: a scalable and efficient approach. EURASIP Journal on Information Security, 2025(1), 28.
29. Chen, Z., & Zhu, H. (2025, January). Secure Net: A Hybrid CNN-LSTM-based Intrusion Detection System for Securing IoT Networks. In Proceedings of the 4th International Conference on Computer, Artificial Intelligence and Control Engineering (pp. 537-544).
30. Dalla, L. O. B., Karal, O., & Degirmenciyi, A. (2025). Leveraging LSTM for Adaptive Intrusion Detection in IoT Networks: A Case Study on the RT-IoT2022 Dataset implemented on a CPU Computer Device Machine.