Bulletin of Electrical Engineering and Informatics
Vol. 15, No. 1, February 2026, pp. 546~556
ISSN: 2302-9285, DOI: 10.11591/eei.v15i1.11046

An intelligence framework for threat detection and response in cloud–IoT-assisted enterprise environments

Amith Shekhar Chandrashekhar[1], Sarala D V[2], Ambuja K[2], Rajani Kallhalli Channarayappa[3], Karanam Sunil Kumar[4]

[1]Department of Computer Science and Engineering, BNM Institute of Technology, Bangalore, India
[2]Department of Computer Science and Engineering, BMS College of Engineering, Bangalore, India
[3]Department of Computer Science and Engineering, East Point College of Engineering and Technology, Bangalore, India
[4]Department of Computer Science and Engineering, R.V. College of Engineering, Bengaluru, India

Article Info

Article history:

Received Jul 16, 2025
Revised Oct 11, 2025
Accepted Dec 6, 2025

Keywords:

Anomaly detection
Cloud–internet of things security
Cyberattack
Response mechanism
Threat intelligence

ABSTRACT

Cloud-internet of things (IoT)-enabled enterprise environments have become an integral part of modern infrastructures, but their increasing interconnectedness makes them vulnerable to sophisticated and rapidly evolving cyber threats. Existing methods for intrusion detection and threat intelligence often suffer from limitations such as high false alarms, low adaptability to new attacks, and computational overhead. To address these challenges, this paper presents an intelligent hybrid framework for threat detection and response in cloud-IoT-enabled enterprises. The proposed system adopts a two-stage architecture: an autoencoder (AE)-based anomaly detector serves as the first security layer to identify deviations from normal traffic behavior, while a convolutional neural network-long short-term memory (CNN-LSTM) model with an attention mechanism serves as the second layer to classify known attack categories with high accuracy. A response mechanism is further integrated to log events, assign severity scores, apply automated protections, and generate real-time alerts, transforming detection into proactive prevention. The system has been evaluated on the benchmark CSE-CIC-IDS2018 dataset, where the anomaly detector achieved an accuracy of 98.4% with a false positive rate of 2%, while the CNN-LSTM-Attention intrusion classifier achieved an accuracy of 99.42%.

Corresponding Author:

Amith Shekhar Chandrashekhar
Department of Computer Science and Engineering, BNM Institute of Technology
Banashankari Stage II, Banashankari, Bengaluru, Karnataka 560070, India
Email: amith_shekhar@bnmit.in

1. INTRODUCTION

The rapid adoption of cloud-internet of things (IoT)-enabled enterprise environments has enabled organizations to provide scalable services and support diverse applications, from smart healthcare to industrial automation. However, this interconnectedness also increases the attack surface, leaving critical infrastructure exposed to sophisticated cyber threats [1]. Vulnerabilities can arise from a variety of factors, including weak access controls, insecure IoT devices, misconfigurations in cloud services, and insufficient visibility into resource utilization. In such circumstances, adversaries exploit these weaknesses to launch distributed denial of service (DDoS), brute-force attacks, intrusions, and web-based attacks, which can severely disrupt services and compromise sensitive data [2]. Furthermore, the dynamic nature of IoT traffic, combined with flexible and multi-tenant cloud environments, poses significant challenges to designing

effective security solutions. The traditional rule-based intrusion detection systems often fail to adapt to emerging threats, while machine learning (ML)-based methods struggle with imbalanced datasets, scalability issues, and detecting previously unseen (zero-day) attacks [3]. As a result, researchers are increasingly turning to intelligent hybrid frameworks that combine anomaly detection, deep learning (DL) models, and automated response mechanisms to ensure robust and proactive cybersecurity in such enterprise ecosystems [4], [5].

In recent years, several research works have been presented in the literature to address the need for intelligent security mechanisms in cloud and IoT-integrated infrastructures. The work done by Tuyishime *et al*. [6] suggested a proactive threat monitoring approach that improved detection timeliness, but it also suffered from large-scale data noise. Similarly, Zacharis *et al.* [7] explored AI-driven threat intelligence for forecasting cyber incidents, which showed improved adaptability in training exercises. Xiao [8] designed a malware cyber threat intelligence framework for IoT using ML models, which enhanced malware identification but has low generalization to unseen traffic due to the class imbalance issue in the dataset. Lilhore *et al*. [9] introduced a hybrid learning framework with a zero-trust architecture for cloud threat detection with strong accuracy, but also requires extensive computing resources. Spyros *et al.* [10] further contributed an AI-based framework for cyber-threat intelligence management, which provided a comprehensive intelligence approach but incurred heavy computational overhead. The application of the blockchain has also gained attention as a tool for strengthening trust in distributed infrastructures. The work of Park and Park [11] developed a blockchain-based trust measurement system for IoT devices, which improved authenticity but suffered from increased latency. Erukala *et al*. [12] introduced a consortium blockchain for smart homes, enhancing privacy but with limited scalability. Shan *et al.* [13] applied blockchain-based service networks to public IT systems. Similarly, Subramanian *et al.* [14] presented blockchain with reinforcement learning for secure task offloading in 5G edge networks, and achieved dynamic adaptability but at higher computational costs. Gil and Arayici [15] applied a random forest (RF) classifier for cultural heritage data segmentation, while Bakro *et al.* [16] combined bio-inspired feature selection with RF for cloud-IDS, improving detection rates but demanding significant feature engineering. Ramachandran *et al*. [17] used a hybrid model for achieving better efficiency yet at the expense of interpretability. Norouzi *et al*. [18] and Al-Abadi *et al.* [19] extended their work to medical IoT networks towards enhancing intrusion detection, but it requires extensive labelled datasets. Attou *et al*. [20] evaluated ML-based cloud IDS and reported reasonable accuracy but high false positive rates. The incorporation of DL with federated learning (FL) have also been introduced by researchers to preserve data privacy in cloud environments. Wang *et al*. [21] presented a verifiable FL framework that secured distributed training but increased communication costs. Landman and Nissim [22] proposed a Linux-specific FL system, effective against malware but with overhead from privacy-preserving mechanisms. Kalimumbalo *et al*. [23] introduced a hybrid model for cloud infrastructures, which improved scalability but suffered synchronization delays. Huang *et al*. [24] designed a personalized FL for cyber intrusion detection, and claimed accuracy gains but higher training complexity. Lytvyn and Nguyen [25] worked on secure multi-party FL for network monitoring, which enhanced collaboration but introduced vulnerability to poisoning attacks.

The identified research problem are as follows: i) existing threat intelligence approaches suffer from integration complexity, making it difficult to align with heterogeneous cloud–IoT enterprise workflows and existing security tools; ii) existing blockchain methods suffers from increased latency and higher demands of storage owing to adoption of consensus protocol, iii) traditional ML models are not much adaptive to dynamic intrusion scenarios and exhibit strong dependence on large volumes of labeled data; and iv) the widely adopted FL in DL methods is susceptible to data leakage, inference attack, and model poisoning while it also calls for complexity in implementation right from aggregation, synchronization, and update management. Hence, there is a need to evolve with a novel strategy that combines simplified implementation with robust security encapsulating the cloud from various potential attacks.

The proposed study aims to present an intelligent threat detection and response framework that improves security performance in cloud-IoT-assisted enterprise environments exposed to diverse and dynamic cyberattacks. The key contributions of this work are: i) a two-step detection approach is designed, where an autoencoder (AE)-based anomaly detector trained on benign traffic identifies deviations from normal behavior, allowing suspicious traffic flows to be filtered before forwarding them for detailed analysis; ii) a hybrid convolutional neural network-bidirectional long short-term memory (CNN-BiLSTM)-attention intrusion classifier is proposed to accurately classify anomalous traffic into specific attack classes, leveraging convolutional layers for spatial feature extraction, recurrent layers for temporal dependency modeling, and multi-head attention to capture global context relationships; and iii) an automated response mechanism is integrated to log events, perform severity tagging, enforce traffic control, and issue real-time alerts, thereby transforming the framework from purely detection to intrusion prevention. The novelty of the proposed approach is the multi-layered security approach that provides comprehensive protection features against both unknown and known attacks along with an automated response mechanism.

2. METHOD

The proposed study aims to present an intelligent threat detection and response framework that improves security performance in cloud-IoT-assisted enterprise environments exposed to diverse and dynamic cyberattacks. The proposed system includes an AE-based anomaly detector trained on benign traffic for early zero-day threat detection and a CNN-BiLSTM with an attention intrusion classifier that accurately classifies malicious traffic into different attack types. A response mechanism complements the detection by providing a threat score that integrates anomaly severity, classification probability, and contextual risk. Based on the score, the system performs activities such as event logging, severity tagging, traffic rate limiting, automatic isolation of affected devices, and administrator alerting. The proposed system design ensures robust, real-time, and context-sensitive security for enterprise cloud infrastructures integrated with IoT systems. The system is not only scalable to large traffic volumes but also adapts to changing attack patterns, providing stronger resilience than traditional IDS approaches. Figure 1 shows the overall architecture of the proposed system, which integrates three main modules: data preprocessing and feature engineering, a two-layer detection system, and a response system.

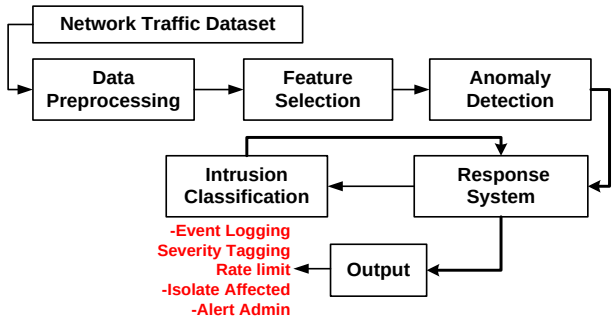

Figure 1. Methodological representation of the proposed scheme

2.1. Dataset description

This study uses the CSE-CIC-IDS2018 dataset [26], a widely adopted standard for intrusion detection in enterprise and IoT-cloud environments. This dataset contains over 6.6 million flow records and 78 features, covering both benign traffic and various types of attacks such as DoS, DDoS, brute force, web-based exploits, botnet activities, and intrusion attempts. To improve clarity and reduce fragmentation of attack classes, we implemented an attack mapping strategy that combined similar attacks into broader categories (for example, grouping multiple DoS types into "DoS," DDoS types into "DDoS," and web-based attacks into "WebAttack"). This mapping reflects realistic enterprise scenarios and ensures balanced evaluation across semantically consistent categories. Table 1 presents the dataset classes after mapping into common groupings.

Table 1. Highlights attack category distribution in CSE-CIC-IDS2018 (after mapping)

Class	Records	Examples of original labels
Benign	5,329,008	Benign traffic
DDoS	775,955	DDoS-LOIC-HTTP, HOIC, and LOIC-UDP
DoS	196,568	Hulk, GoldenEye, Slowloris, and SlowHTTPTest
Bot	144,535	Botnet activity
Infiltration	118,483	Infiltration
BruteForce	94,330	FTP, SSH, and XSS brute force
WebAttack	653	SQL Injection and Brute Force-Web
Total	6,659,532	—

After mapping of attack labels, the dataset was split into training (70%), validation (15%), and test (15%) sets using stratified sampling to maintain class proportions. This ensures that the learning process receives representative samples from all attack categories while also preserving unseen data for unbiased evaluation. Despite the class imbalance (e.g., very few WebAttack records), this distribution reflects real-world network traffic, making the dataset suitable for evaluating intrusion detection in cloud-IoT-assisted enterprise environments.

2.2. Data preprocessing

The raw dataset consisted of 78 features extracted from bidirectional network flows. Since initial inspection revealed no missing values, the preprocessing pipeline focused on standardization, feature reduction, and transformation to ensure robust learning. All numerical features were scaled using z-score normalization so that features in different categories (e.g., packet count vs. duration value) contribute equally to the learning process. To further improve the feature representation, principal component analysis (PCA) was applied to the training set, retaining 95% of the variance. This transformation method reduced the dimensionality to 24 principal components, effectively eliminating redundancy while preserving the most informative patterns. The same transformation was also consistently applied to the validation and test sets to ensure comparability.

2.3. Anomaly detector

The anomaly detector forms the first security layer of the proposed system and is designed to identify deviations from normal traffic behaviour before forwarding the data to the intrusion classifier. To capture the underlying statistical distribution of legitimate flows in cloud-IoT-assisted environments, an AE architecture was used, trained only on benign traffic samples. Here, traffic that could not be accurately reconstructed by the AE was considered anomalous, indicating potential malicious activity. The autoencoder's architecture is symmetric, as shown in Figure 2, consisting of an encoder that compresses the input into a latent representation and a decoder that reconstructs it.

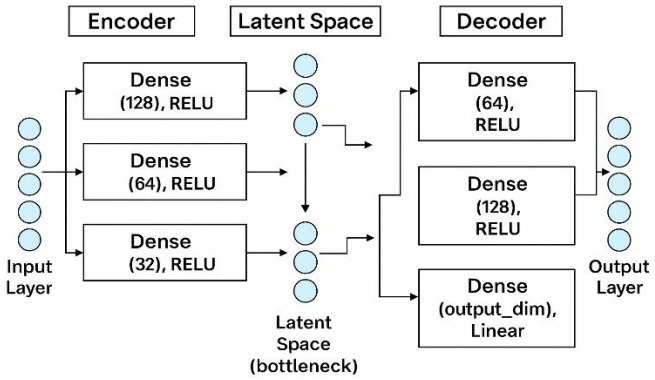

Figure 2. Illustrates the architecture of the adopted AE network architecture

The proposed AE network consists of an initial layer, called the input layer, which holds a transformed feature vector obtained from preprocessing and feature transformation operations. The encoder layer of the network is composed of three fully connected dense layers of decreasing dimensionality. The first dense layer consists of 128 neurons with rectified linear units (ReLU) activation, followed by a second dense layer of 64 neurons with ReLU activation, and finally a third dense layer of 32 neurons with ReLU activation. This creates a bottleneck latent space, which provides the densest and informative representation of benign traffic patterns. The decoder is designed symmetrically to the encoder, reconstructing the original feature space using a dense layer of 64 neurons with ReLU activation, followed by another dense layer of 128 neurons with ReLU activation. The final reconstruction is performed by an output dense layer that matches the original input dimension and uses a linear activation function. During the training phase, the AE is optimised using the mean square error (MSE) between the input and reconstructed vectors as the loss function. An Adam optimizer with a learning rate of 0.001 is considered, and training is conducted for 50 epochs with a batch size of 256. Anomaly detection was based on the reconstruction error.

2.4. Intrusion detection

The second layer of the proposed framework is a hybrid DL classifier that integrates CNN, BiLSTM units, and a multi-head self-attention (MHSA) mechanism to provide fine-grained classification of suspicious traffic already filtered by the anomaly detector. This stage of the system implementation focuses on combining spatial, temporal, and attention-based feature extraction to provide robust multi-class classification of intrusions in cloud-IoT-assisted environments. Figure 3 shows the schematic layout of the CNN-BiLSTM with the attention model.

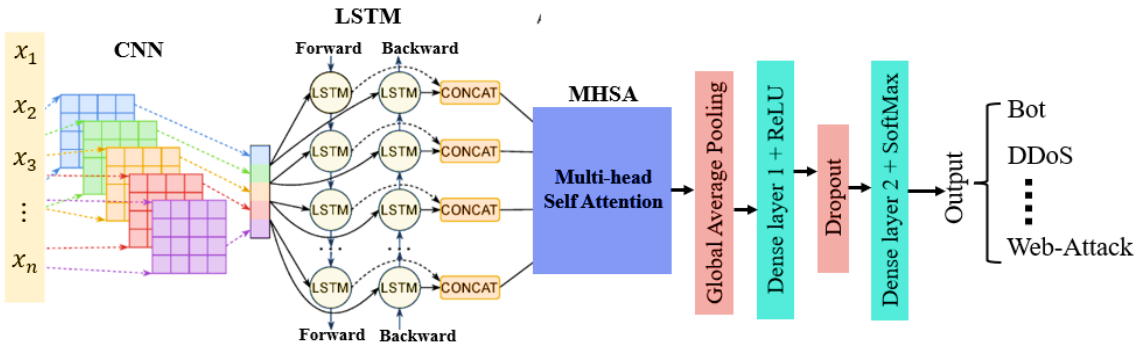

Figure 3. A schematic outline of the proposed CNN-LSTM attention model for intrusion detection

As shown in Figure 3, the first layer of the proposed IDS model is a 1D CNN layer that applies convolutional filters to capture local spatial dependencies between features. This block consists of two convolutional layers with 64 filters (kernel size=3, activation=ReLU), followed by a max-pooling layer and a dropout layer (0.3) to prevent overfitting. The extracted feature maps are then fed into a BiLSTM layer with 64 units, which processes traffic flow in both forward and backward directions to capture sequential dependencies. The output of the BiLSTM passes through an MHSA module, which highlights the most important features for classification and also incorporates a residual correlation and standardization for stability. After attention, a global average pooling layer condenses the temporal features into a concise representation. Finally, two fully connected layers perform the classification: a dense layer of 128 neurons with ReLU activation and dropout (0.3), followed by a softmax output layer with the same number of neurons as the number of traffic categories. The layer-wise configuration of the CNN-BiLSTM with the attention model is highlighted in Table 2.

Table 2. Presents model configuration of CNN–BiLSTM with attention classifier

Layer type	Configuration details
Input layer	PCA-transformed feature vector reshaped to (24, 1)
Conv1D layer 1	64 filters, kernel size=3, activation=ReLU, and padding=same
Conv1D layer 2	64 filters, kernel size=3, activation=ReLU, and padding=same
MaxPooling1D	Pool size=2
Dropout	Rate=0.3
BiLSTM layer	64 units, return sequences=true (forward+backward concatenation)
Multi-head self-attention	4 heads, key dimension=64, and residual connection+layer normalization
Global average pooling	Reduces sequence to compact representation
Dense layer 1	128 neurons, activation=ReLU
Dropout	Rate=0.3
Dense output layer	Neurons=number of classes (7), activation=Softmax

The model was trained using the Adam optimizer with a fixed learning rate of 0.001. The sparse categorical cross-entropy loss function was used since the problem involves multi-class classification with integer-encoded labels. Training was conducted for 30 epochs with a batch size of 256, and the validation set was used to monitor generalization performance during training. Dropout regularization was employed to reduce overfitting, while early stopping was considered to avoid unnecessary iterations once convergence was achieved.

2.5. Response mechanism

The final stage of the proposed framework incorporates an automated response system that generates to provide actionable defence measures to mitigate severe damages in cloud–IoT-assisted enterprise environments. The proposed response system performs four essential functions. Firstly, when the proposed anomaly detection model identifies any anomalous event in the incoming network traffic, the response system logs this event and immediately activates the second line of defence, i.e., CNN-LSTM-Attention model to classify known threats. Upon classification or identification of known threats, the response system again logs the event and ensures that every intrusion attempt and detection outcome is stored for auditing, forensic analysis, and model retraining. It also performs severity tagging, which assigns a criticality score based on the attack category, confidence score of the model and frequency of attack event,

which allows administrators to prioritise high-risk alerts such as DDoS or infiltration over low-severity brute-force attempts. Third, the response system can also enforce real-time traffic controls, such as rate limiting suspicious flows and isolating compromised IoT devices from the enterprise cloud network, thereby containing the attack before it spreads. Finally, the system issues administrative alerts, providing real-time notifications to network operators for immediate human intervention when required. Algorithm 1 describes the working process of the proposed response mechanisms in the cloud–IoT-assisted enterprise environments.

Algorithm 1. Application of the proposed response mechanism

```
Input: Incoming network traffic flow
Output: Event log, classification result, and triggered defence action
Start
    1.  For each incoming traffic flow F:
    2.      Pass F to Anomaly Detector (Autoencoder)
    3.      If reconstruction error ≤ threshold:
    4.          Mark F as Benign, forward traffic, and log event
    5.      Else:
    6.          Mark F as Anomalous, log event
    7.          Forward F to CNN–LSTM–Attention Classifier
    8.          Obtain predicted attack category C and confidence score P
    9.          Log attack event (C, P) for auditing and forensic analysis
    10.         Perform Severity Tagging:
    11.             If C ∈ {DDoS, Infiltration} or P ≥ severity threshold:
    12.                 Assign High Severity
    13.             Else:
    14.                 Assign Low/Moderate Severity
    15.         Apply Defense Action based on severity:
    16.             If High Severity → Apply rate limiting or isolate device
    17.             If Low Severity → Continue monitoring and logging
    18.         Trigger Administrative Alert for immediate notification
    19. End For
    End
```

3. RESULTS

This section presents the study outcomes accomplished after implementing the proposed study model. The modelling of the proposed security system is done using Python 3.8 with TensorFlow for designing the proposed AE and CNN-LSTM-Attention model. The assessment is carried out by considering standard performance metrics such as overall accuracy, precision, recall and F1-score. The proposed CNN–LSTM with attention model demonstrates strong effectiveness in multi-class intrusion detection on the CSE-CIC-IDS2018 dataset, as can be evident from the confusion matrix in Figure 4 and quantified outcome in Table 3.

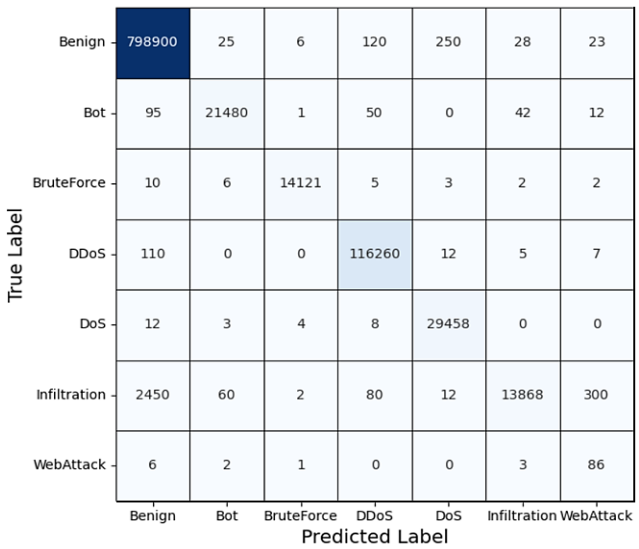

Figure 4. A confusion matrix for intrusion detection

Table 3. The performance analysis of a multi-class intrusion detection system

Class	Precision (%)	Recall (%)	F1-score (%)	Support
Benign	99	100	99	799352
Bot	100	99	99	21680
BruteForce	100	100	100	14149
DDoS	100	100	100	116394
DoS	99	99	99	29485
Infiltration	85	78	81	17772
WebAttack	92	88	90	98
Overall accuracy		99.42		

The confusion matrix in Figure 4 shows that the proposed model correctly classifies the majority of benign and attack traffic with very few errors. For Benign, DDoS, DoS, Bot, and BruteForce traffic, the model achieves near-perfect precision and recall, reflecting the strength of the hybrid design that addresses both volumetric and authentication-based threats. Table 3 further validates this robustness, reporting an overall accuracy of 99.42%. For minority attack classes such as WebAttack and Infiltration, recall values of 0.88 and 0.78 are observed. These results highlight the persistent challenge of class imbalance in real-world network traffic. Nonetheless, the overall analysis confirms that the CNN–LSTM with Attention model effectively captures spatial and temporal dependencies in the data and delivers high classification accuracy. The performance of the AE as an anomaly detector is presented in Figure 5 and Table 4. The AE also demonstrates strong capability in identifying anomalies by learning normal patterns and flagging deviations, and ensures that only suspicious flows are passed to the CNN–LSTM with Attention classifier, thereby reducing processing overhead and enabling the overall framework to operate as an integrated two-layer defence system.

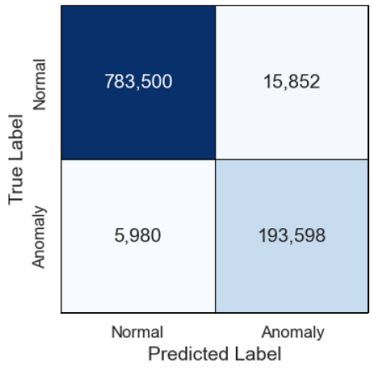

Figure 5. A confusion matrix for anomaly detection

Table 4. Performance metrics of the AE for anomaly detection

Class	Precision (%)	Recall (%)	F1-score (%)	Support
Normal	99.0	98.0	99.0	799352
Anomaly	96.0	97.0	97.0	199578
Accuracy		98.5		998930

The confusion matrix in Figure 5 shows that the majority of normal flows are correctly reconstructed with low reconstruction error, while a significant proportion of anomalous flows are also detected. This outcome reflects the ability of the model to generalise beyond training data. The performance metrics in Table 4 confirm that the AE achieves 98.5% overall accuracy with strong precision and recall values across both classes. Normal traffic is classified with 99% precision and 98% recall, which ensures minimal false positives and prevents unnecessary alerts in deployment. Anomalous traffic reaches 96% precision and 97% recall, confirming that the AE captures deviations and potential zero-day attacks with reliability. The results establish the AE as a dependable first layer of defence, functioning as a lightweight anomaly filter that reduces the volume of traffic forwarded to the secondary IDS for deeper inspection. To further assess effectiveness, Table 5 presents a comparative analysis with existing studies conducted on the CSE-CIC-IDS2018 dataset.

Table 5. A comparison with similar existing work

Reference	Model	Accuracy (%)	F1-score (%)
[27]	RF-based meta model	84	82.7
[28]	Deep autoencoder (DAE)	86	86
[29]	Multibranch hybrid perceptron	95.49	92.38
[30]	CNN+LSTM	92.49	96.14
[31]	LSTM+multi-head attention	81.38	88.29
[32]	LSTM+transformer	92.14	88.35
Proposed anomaly detection	Deep autoencoder (binary)	98.5	98.5
Proposed intrusion detection	CNN–LSTM+attention (multiclass)	99.42	98.81

The comparative analysis in Table 5 highlights the superior performance of the proposed two-layer security framework on the CSE-CIC-IDS2018 dataset. The anomaly detection module (autoencoder) achieved 98.5% accuracy with an F1-score of 0.97, while the multiclass intrusion detection model (CNN–BiLSTM with Attention) attained 99.42% accuracy and a 98.81% F1-score. These results demonstrate consistent improvements over prior works in both anomaly detection and multiclass classification. The earlier approaches reported lower effectiveness: Oleiwi *et al*. [27] applied a RF meta-model with 84% accuracy, showing limited generalization; Mhawi *et al*. [28] used DAE with 86% accuracy but lacked hybrid spatial–temporal modelling; and Al-Khayyat and Ucan [29] achieved 95.49% accuracy and 0.9238 F1 with a hybrid perceptron, yet performance dropped in multi-class scenarios. Similarly, Hnamte *et al.* [30] (CNN+LSTM, 92.49% accuracy, 0.9614 F1) and Zhu *et al.* [32] (LSTM+transformer, 92.14% accuracy, 0.8835 F1) improved detection but struggled with imbalanced classes such as WebAttack and Infiltration. Cai *et al.* [31] explored multi-head attention for feature integration, but scalability issues limited accuracy to 81.38%. The reason behind achieving better performance by the proposed system is its architecture that includes PCA-based feature optimization, which reduces noise and redundancy, the hybrid CNN–BiLSTM extracts both spatial and temporal dependencies, and the attention layer focuses on critical traffic features, which improves detection of rare attacks. To further validate the effectiveness of each component in the proposed framework, a sensitivity analysis was performed, as shown in Table 6.

Table 6. Sensitivity analysis of proposed model components

Model variant	Accuracy (%)	F1-score (%)
CNN only	95.62	93.8
CNN+Bi-LSTM	97.84	96.5
CNN+Bi-LSTM+attention	99.42	99.09
Autoencoder (anomaly detection only)	98.50	97.0
Two-layer (autoencoder+CNN–LSTM–attention)	99.42	99.81

4. CONCLUSION

This study introduced an intelligence-driven two-layer intrusion detection framework tailored for IoT–cloud-assisted enterprise environments. The framework integrates an AE-based anomaly detector as the first defence layer and a hybrid CNN–BiLSTM–Attention model as the second layer for intrusion classification. The AE, trained exclusively on benign traffic, effectively detected abnormal patterns, including previously unseen zero-day attacks. The proposed framework demonstrates strength through its layered architecture and PCA-based dimensionality reduction, which removes redundant features while preserving the most informative traffic characteristics. Within the classifier, the CNN module extracts spatial representations of network flows, the BiLSTM captures temporal dependencies, and the attention mechanism emphasises critical features, leading to improved classification of minority attack classes. The proposed security system establishes a resilient defence solution capable of handling the dynamic and heterogeneous nature of IoT–cloud networks. Future work will focus on refining the hybridisation process to address multi-colluding dynamic attacks in data centres and extending the approach with FL to enhance scalability and privacy.

FUNDING INFORMATION

The authors state no funding is involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Amith Shekhar Chandrashekhar	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Sarala D V		✓				✓		✓	✓	✓	✓	✓		
Ambuja K	✓		✓	✓			✓			✓	✓		✓	
Rajani Kallhalli Channarayappa	✓			✓	✓		✓	✓	✓	✓	✓			
Karanam Sunil Kumar	✓		✓		✓		✓	✓	✓	✓	✓	✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1] R. Bathini and N. Vurukonda, "A survey to build framework for optimize and secure migration and transmission of cloud data," *Bulletin of Electrical Engineering and Informatics*, vol. 13, no. 2, pp. 812–820, Apr. 2024, doi: 10.11591/eei.v13i2.5181.

[2] M. H. Moharam, O. Hany, A. Hany, A. Mahmoud, M. Mohamed, and S. Saeed, "Anomaly detection using machine learning and adopted digital twin concepts in radio environments," *Scientific Reports*, vol. 15, no. 1, pp. 1-19, May 2025, doi: 10.1038/s41598-025-02759-5.

[3] R. Wang, C. Li, K. Zhang, and B. Tu, "Zero-trust based dynamic access control for cloud computing," *Cybersecurity*, vol. 8, no. 1, pp. 1-16, Feb. 2025, doi: 10.1186/s42400-024-00320-x.

[4] A. Punia, P. Gulia, N. S. Gill, E. Ibeke, C. Iwendi, and P. K. Shukla, "A systematic review on blockchain-based access control systems in cloud environment," *Journal of Cloud Computing*, vol. 13, no. 1, pp.1-37, Sep. 2024, doi: 10.1186/s13677-024-00697-7.

[5] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, "Security of Zero Trust Networks in Cloud Computing: A Comparative Review," *Sustainability*, vol. 14, no. 18, pp. 1-21, Sep. 2022, doi: 10.3390/su141811213.

[6] E. Tuyishime, T. C. Balan, P. A. Cotfas, D. T. Cotfas, and A. Rekeraho, "Enhancing Cloud Security—Proactive Threat Monitoring and Detection Using a SIEM-Based Approach," *Applied Sciences*, vol. 13, no. 22, pp. 1-18, Nov. 2023, doi: 10.3390/app132212359.

[7] A. Zacharis, V. Katos, and C. Patsakis, "Integrating AI-driven threat intelligence and forecasting in the cyber security exercise content generation lifecycle," *International Journal of Information Security*, vol. 23, no. 4, pp. 2691–2710, May 2024, doi: 10.1007/s10207-024-00860-w.

[8] P. Xiao, "Malware Cyber Threat Intelligence System for Internet of Things (IoT) Using Machine Learning," *Journal of Cyber Security and Mobility*, vol. 13, no. 1, pp. 1-18, Dec. 2023, doi: 10.13052/jcsm2245-1439.1313.

[9] U. K. Lilhore *et al.*, "SmartTrust: a hybrid deep learning framework for real-time threat detection in cloud environments using Zero-Trust Architecture," *Journal of Cloud Computing*, vol. 14, no. 1, pp. 1-37, Jul. 2025, doi: 10.1186/s13677-025-00764-7.

[10] A. Spyros *et al.*, "AI-Based Holistic Framework for Cyber Threat Intelligence Management," *IEEE Access*, vol. 13, pp. 20820–20846, 2025, doi: 10.1109/access.2025.3533084.

[11] J. Park and S. Park, "TM-Chain: TCB Measurement Management Using Cloud Blockchain for IoT Devices," *IEEE Access*, vol. 13, pp. 8941–8950, 2025, doi: 10.1109/access.2025.3525807.

[12] S. B. Erukala, D. Tokmakov, A. D. Aguru, R. Kaluri, A. Bekyarova-Tokmakova, and N. Mileva, "An End-to-End Secure Communication Framework for Smart Homes Environment Using Consortium Blockchain System," *IEEE Access*, vol. 13, pp. 67250–67268, 2025, doi: 10.1109/access.2025.3559070.

[13] Z. Shan, X. Chen, Y. Zhang, Y. He, and D. Wang, "Exploration and Practice of Constructing Trusted Public IT Systems Using Blockchain-Based Service Network," *Tsinghua Science and Technology*, vol. 30, no. 1, pp. 124–134, Feb. 2025, doi: 10.26599/tst.2023.9010159.

[14] N. S. Subramanian, P. Krishnan, K. Jain, K. B. A. Kumar, T. Pandey, and R. Buyya, "Blockchain and RL-Based Secured Task Offloading Framework for Software-Defined 5G Edge Networks," *IEEE Access*, vol. 13, pp. 56820–56842, 2025, doi: 10.1109/access.2025.3554638.

[15] A. Gil and Y. Arayici, "Point Cloud Segmentation Based on the Uniclass Classification System with Random Forest Algorithm

for Cultural Heritage Buildings in the UK," *Heritage*, vol. 8, no. 5, pp. 1-20, Apr. 2025, doi: 10.3390/heritage8050147.
[16] M. Bakro *et al.*, "Building a Cloud-IDS by Hybrid Bio-Inspired Feature Selection Algorithms Along With Random Forest Model," *IEEE Access*, vol. 12, pp. 8846–8874, 2024, doi: 10.1109/access.2024.3353055.
[17] D. Ramachandran, M. Albathan, A. Hussain, and Q. Abbas, "Enhancing Cloud-Based Security: A Novel Approach for Efficient Cyber-Threat Detection Using GSCSO-IHNN Model," *Systems*, vol. 11, no. 10, pp. 1-30, Oct. 2023, doi: 10.3390/systems11100518.
[18] M. Norouzi, Z. Gürkaş-Aydın, Ö. C. Turna, M. Y. Yağci, M. A. Aydin, and A. Souri, "A Hybrid Genetic Algorithm-Based Random Forest Model for Intrusion Detection Approach in Internet of Medical Things," *Applied Sciences*, vol. 13, no. 20, pp. 1-14, Oct. 2023, doi: 10.3390/app132011145.
[19] A. A. J. Al-Abadi, M. B. Mohamed, and A. Fakhfakh, "Enhanced Random Forest Classifier with K-Means Clustering (ERF-KMC) for Detecting and Preventing Distributed-Denial-of-Service and Man-in-the-Middle Attacks in Internet-of-Medical-Things Networks," *Computers*, vol. 12, no. 12, pp. 1-16, Dec. 2023, doi: 10.3390/computers12120262.
[20] H. Attou, A. Guezzaz, S. Benkirane, M. Azrour, and Y. Farhaoui, "Cloud-Based Intrusion Detection Approach Using Machine Learning Techniques," *Big Data Mining and Analytics*, vol. 6, no. 3, pp. 311–320, Sep. 2023, doi: 10.26599/bdma.2022.9020038.
[21] H. Wang, T. Yang, Y. Ding, S. Tang, and Y. Wang, "VPPFL: Verifiable Privacy-Preserving Federated Learning in Cloud Environment," *IEEE Access*, vol. 12, pp. 151998–152008, 2024, doi: 10.1109/access.2024.3472467.
[22] T. Landman and N. Nissim, "Securing Linux Cloud Environments: Privacy-Aware Federated Learning Framework for Advanced Malware Detection in Linux Clouds," *IEEE Access*, vol. 13, pp. 30377–30394, 2025, doi: 10.1109/access.2025.3540955.
[23] D. M. Kalimumbalo *et al.*, "SecFedMDM-1: A Federated Learning-Based Malware Detection Model for Interconnected Cloud Infrastructures," *IEEE Access*, vol. 13, pp. 101246–101261, 2025, doi: 10.1109/access.2025.3577706.
[24] X. Huang, J. Liu, Y. Lai, B. Mao, and H. Lyu, "EEFED: Personalized Federated Learning of Execution&Evaluation Dual Network for CPS Intrusion Detection," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 41–56, 2023, doi: 10.1109/tifs.2022.3214723.
[25] O. Lytvyn and G. Nguyen, "Secure Federated Learning for Multi-Party Network Monitoring," *IEEE Access*, vol. 12, pp. 163262–163284, 2024, doi: 10.1109/access.2024.3486810.
[26] A. Mohamed, "CSE-CIC-IDS2018," *Mendeley Data*, 2024, doi: 10.17632/29hdbdzx2r.1.
[27] H. W. Oleiwi, D. N. Mhawi, and H. Al-Raweshidy, "A Meta-Model to Predict and Detect Malicious Activities in 6G-Structured Wireless Communication Networks," *Electronics*, vol. 12, no. 3, pp. 1-15, Jan. 2023, doi: 10.3390/electronics12030643.
[28] D. N. Mhawi, H. W. Oleiwi, and H. Al-Raweshidy, "Towards Intelligent Threat Detection in 6G Networks Using Deep Autoencoder," *Electronics*, vol. 14, no. 15, pp. 1-17, Jul. 2025, doi: 10.3390/electronics14152983.
[29] A. T. K. Al-Khayyat and O. N. Ucan, "A Multi-Branched Hybrid Perceptron Network for DDoS Attack Detection Using Dynamic Feature Adaptation and Multi-Instance Learning," *IEEE Access*, vol. 12, pp. 192618–192638, 2024, doi: 10.1109/access.2024.3508028.
[30] V. Hnamte, A. A. Najar, H. Nhung-Nguyen, J. Hussain, and M. N. Sugali, "DDoS attack detection and mitigation using deep neural network in SDN environment," *Computers & Security*, vol. 138, p. 103661, Mar. 2024, doi: 10.1016/j.cose.2023.103661.
[31] M. Cai, J. Zhan, C. Zhang, and Q. Liu, "Fusion k-means clustering and multi-head self-attention mechanism for a multivariate time prediction model with feature selection," *International Journal of Machine Learning and Cybernetics*, vol. 16, no. 12, pp. 9979–9997, Dec. 2024, doi: 10.1007/s13042-024-02490-z.
[32] C. Zhu, X. Ma, P. D'Urso, Y. Qian, W. Ding, and J. Zhan, "Long-Term Multivariate Time-Series Forecasting Model Based on Gaussian Fuzzy Information Granules," *IEEE Transactions on Fuzzy Systems*, vol. 32, no. 11, pp. 6424–6438, Nov. 2024, doi: 10.1109/tfuzz.2024.3449769.

BIOGRAPHIES OF AUTHORS

Amith Shekhar Chandrashekhar is currently working as associate professor in Department of Computer Science and Engineering at BNM Institute of Technology, Bangalore. He earned his Ph.D. in Computer Science and Engineering from RVCE, Visvesvaraya Technological University (VTU), Belagavi, in 2023. He received his Master of Technology (M.Tech.) degree from BIET, VTU, Belagavi, in 2012, and Bachelor of Engineering (B.E.) from GMIT, VTU, Belagavi, in 2009. He has 14 years of academic experience. He has published more than 10+ research articles in international journals and conference proceedings. His research interest includes cloud computing and machine learning. He can be contacted at email: amith_shekhar@bnmit.in.

Sarala D V is currently serving as an assistant professor in the Department of Computer Science and Engineering at BMS College of Engineering, Bangalore. She earned her Ph.D. in Computer Science and Engineering from Visvesvaraya Technological University (VTU), Belagavi. She received her Master's of Technology (M.Tech.) degree in the field of Computer Science and Engineering from VTU, Belagavi in 2012 and Bachelor of Engineering (B.E) degree in the field of Computer Science and Engineering from VTU, Belagavi, in 2010. She has contributed to the academic community by publishing in many international journals/conferences. Her area of interest includes computer vision, machine learning, and deep learning. She can be contacted at email: saraladv.cse@bmsce.ac.in.

Ambuja K is currently working as an assistant professor in Department of Computer Science and Engineering at BMS College of Engineering (BMSCE)**,** Bangalore. She received her Masters of Technology (M.Tech.) degree in Computer Science and Engineering from BNMIT, Visvesvaraya Technological University (VTU), Belagavi, in 2018, and Bachelor of Engineering (B.E.) degree in Computer Science and Engineering from CBIT, VTU, Belagavi, in 2016. She has 5 years of academic experience. Also, she is pursuing her Ph.D. degree from VTU Belagavi. Her research interest includes image processing, artificial intelligence, and machine learning. She can be contacted at email: ambuja.cse@bmsce.ac.in.

Rajani Kallhalli Channarayappa is an associate professor in Department of Computer Science and Engineering at the East Point College of Engineering and Technology, K R Puram, Bangalore at Visvesvaraya Technological University (VTU), Belagavi. She completed Bachelor of Engineering (B.E.) from NCET, and Master of Technology (M.Tech.) from Atria Institute of Technology. She has many publications on isolating routing misbehavior problems in mobile ad hoc networks. She had more than 8 years of teaching experience and worked as an assistant professor in various colleges like NCET, SRSIT, and Presidency University. Her vision is to be a successful teacher by incorporating good teaching values and to provide students a quality in teaching. Her research interest focuses on mobile ad-hoc networks, wireless sensor networks, WANET'S, and machine learning. He can be contacted at email: rajanikcc009@gmail.com.

Karanam Sunil Kumar is currently serving as an assistant professor at RV College of Engineering. He completed his Bachelor of Engineering (B.E.), Master of Technology (M.Tech.), and Ph.D. from Visvesvaraya Technological University (VTU), Belagavi. With a career spanning 16 years, he has a wealth of experience in his field. He has contributed to the academic community by publishing six papers, which have been indexed in top-tier categories ranging from Q1 to Q4. His research interests are computer vision, machine learning, big data, and deep learning. He can be contacted at email: ksunilkumar@rvce.edu.in.