A Performance Analysis of ML-Based Intrusion Detection Systems in Cloud Environments

Khatha Mahendar and Gandla Shivakanth*
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad, India
Email: mahendarkatha@gmail.com (K.M.), shvkanth0@gmail.com (G.S.)

Manuscript received March 27, 2025; revised May 13, 2025; accepted May 29, 2025
*Corresponding author

***Abstract*—Intrusion Detection Systems (IDS) are important for protecting cloud environments against emerging cyber threats. This paper introduces AI-SCAN (artificial intelligence-driven scalable convolutional network for anomaly detection in cloud networks), a deep learning IDS that utilizes a Convolutional Neural Network (CNN) architecture to achieve better threat detection with better scalability, flexibility, and low false positives. The proposed system overcomes key challenges of dataset bias, external validation, and class imbalance to provide robust performance in dynamic cloud networks. To reduce dataset bias, we examine model performance on a variety of attack types and assess its efficacy with external validation on separate datasets outside the CSE-CICIDS2018 benchmark. Our solution combines SMOTE (synthetic minority oversampling technique)-based data augmentation and class weighting strategies to counteract minority attack classes, promoting model generalization. Hyperparameter tuning and feature selection also improve AI-SCAN's efficiency, reducing computational overhead without sacrificing high detection accuracy. Empirical observations indicate 97.5% accuracy, 96.5% precision, and 95.0% recall, higher than conventional ML-based IDS implementations. AI-SCAN's novel cyber threat detection with low false positives supports its applicability in real-time cloud deployment. The current study conducts a comparative analysis among conventional machine learning (ML), ensemble learning, and deep learning-based IDS models and positions AI-SCAN as a robust, scalable, and fault-tolerant cybersecurity measure.**

***Index Terms*—class imbalance handling, Convolutional Neural Network (CNN), Cloud security, cyber threat detection, dataset bias mitigation, Deep Learning (DL), Explainable AI (XAI), external validation, Intrusion Detection System (IDS), real-time threat detection**

I. Introduction

Intrusion Detection Systems (IDSs) are widely recognized as critical tools for safeguarding computer networks against malicious activity, including hacking or unauthorized access. IDSs scan network environments and can detect unusual behaviors that can help remove potential threats. Nevertheless, conventional IDSs, particularly those employing network-based methods, have inherent weaknesses, including the consistently high rate of false positives of normal and benign activities as malicious. This generates a massive volume of false alarms that can overwhelm analysts, wasting time and diminishing productivity. In worst cases, this number of spurious alarms might slow down and delay the effective detection and reaction to real threats, enabling the attackers to take advantage of the same vulnerabilities. The constraints of conventional IDSs in addressing these problems indicate a critical need for more responsive and efficient detection mechanisms, particularly Machine Learning (ML) based ones for better performance [1, 2].

While traditional IDSs rely primarily on signature-based detection, which is effective against established threats, they struggle to detect new and emerging cyberattacks. Signature-based techniques cannot identify polymorphic malware or zero-day attacks since they depend on established patterns. To achieve this, several machine learning methods have been experimented with for IDS applications, such as decision trees, Support Vector Machines (SVMs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, and Convolutional Neural Networks (CNNs). Nevertheless, each of these methods comes with trade-offs: while decision trees and SVMs are interpretable, they tend to be less scalable in dynamic cloud environments. RNNs and LSTMs learn sequential patterns but are hindered by long training times and higher computational costs. CNN-based IDS models have proved to be more accurate and scalable and are therefore better suited for high-traffic cloud environments [3].

While much progress has been made with IDS technology, contemporary systems continue to struggle in terms of detection and response. The false positive rates are very high, and the most important issue, that normal network activities create many alarms that tend to draw security personnel's attention away from actual risks. Most of the existing IDSs are also based on signature-based detection models that are inherently reactive and incapable of detecting new attack patterns. The binary classification nature of IDS models also serves to emphasize a crucial shortcoming: the inability to classify several kinds of attacks together in complicated network environments. As cloud-based networks are confronted by an ever-changing and unpredictable security threat, analyzing and comparing various ML-based IDS models becomes significant for determining the most suitable detection method [4].

Another major problem with current IDS solutions is the absence of dynamic flexibility. Cyber-attacks become

doi: 10.18178/ijeetc.14.4.243-252

more sophisticated at a fast pace, and security mechanisms need to adapt accordingly without needing constant manual interventions. Conventional ML-based IDS solutions are primarily static and do not self-update to counter new attack techniques without retraining. Attackers exploit this inflexibility to bypass detection mechanisms, increasing the chances of being under cyber-attack for a long time. An effective IDS for cloud environments in real-world scenarios must dynamically learn from network traffic data, increasing its detection capability over time without producing false positives [5, 6].

Another problem associated with ML-based IDS models is their "black box" nature, which reduces transparency and makes it harder to interpret and trust model decisions. For example, SVMs and deep learning models such as LSTMs and CNNs are generally unexplainable, making it harder to verify their detection outcomes. Without interpretability, security analysts may struggle to distinguish between actual threats and false positives. This explainability deficiency has generated growing interest in hybrid strategies that integrate rule-based reasoning and ML-based detection to enhance trust and reliability [7].

The advent of Internet of Things (IoT) technologies and cloud infrastructure makes the challenges of IDS even more challenging. Cloud infrastructures handle large volumes of diverse data, further complicating traffic analysis. Furthermore, emerging attack vectors like Distributed Denial of Service (DDoS) attacks, botnets, and traffic manipulation methods call for IDS products that can efficiently analyze massive cloud traffic. Most current IDSs, especially those based on traditional ML methods, find it difficult to meet such scalability demands, and real-time threat detection within cloud environments is thus challenging [8].

One of the most important features of ML-based IDSs is that they can distinguish between active and passive attacks. Active attacks like DDoS attacks, message spoofing, and brute-force intrusions are disruptive and require instant action. On the other hand, passive attacks like eavesdropping and traffic analysis are more covert, frequently going unnoticed for long periods. IDS models need to integrate real-time anomaly detection methods that can detect both active and passive threats with minimal false positives and false negatives. Conventional ML models are not able to achieve this balance, and therefore, an extensive analysis of various algorithmic methods needs to be performed to identify the best solution [9, 10].

Despite incremental advancements, existing IDS solutions are still not proficient in classifying several attacks with high precision. Most ML-based IDSs are implemented for binary classification (i.e., malicious vs. benign), which hinders their capability in scenarios where multiple attack types happen concurrently. This necessitates sophisticated multi-class classification methods capable of differentiating among various threat classes, such as brute-force attacks, SQL injections, botnets, and infiltration attempts. Comparative research on ML-based IDS models indicates that CNN-based methods provide a promising avenue because of their better capability to extract spatial and temporal patterns in network traffic. Yet, more comparative analysis is needed to confirm their real-world usability in cloud environments.

The specific problem addressed in this work is the high false positive rate and poor generalization capabilities of existing IDS models when deployed in dynamic, cloud-based environments. These issues limit operational efficiency and lead to missed detections or over-alerting, especially in multi-class, real-time attack scenarios. To overcome these challenges, we introduce an artificial intelligence-driven, scalable convolutional network for anomaly detection in cloud networks (AI-SCAN), an enhanced IDS model that methodically analyzes and contrasts various ML-based detection methods. In contrast to current IDS systems, AI-SCAN includes hyperparameter optimization, class balancing strategies, and deep feature extraction for improved detection efficacy across various types of attacks. This research not only reports the design and assessment of AI-SCAN but also critically examines how it compares with other ML-based IDS models, including random forest, RNNs, LSTMs, and baseline CNN methods. With its emphasis on scalability, flexibility, and precision, AI-SCAN is a big leap in determining the best ML-driven IDS model for cloud infrastructure.

II. Literature Review

The rapid diffusion of IoT technology is creating transformative capabilities that redefine technological platforms and connect devices to bring innovation in numerous sectors. IoT technologies create complex systems for the collection and sharing of data. IoT technologies are used by many businesses to provide automation and optimization in the fields of transportation, healthcare, home automation, and industrial applications. IoT devices are essential to healthcare because they allow for patient condition monitoring, which improves results and reduces costs [8]. Similarly, smart homes depend on IoT to provide better security, efficient energy consumption, and convenience through connected appliances. Industries use IoT in predictive maintenance, asset tracking, and process optimization, which increases productivity and reduces possible losses from equipment failure. In transportation, IoT allows for smart traffic management, fleet coordination, and self-driving vehicles, which increase safety and operational efficiency [11]. These applications underscore the necessity of IoT in advancing society and improving the quality of life. Nevertheless, the large-scale adoption of IoT comes with severe cybersecurity threats.

The fundamental threats to IoT security result from the expansion of the attack surface and, in addition, from the diversity of connected devices. Many IoT devices, having restricted processing abilities, become vulnerable to attacks while being otherwise hard to secure effectively. Common vulnerabilities include poor authentication

protocols, non-encryption, and poor security updates, which make IoT systems vulnerable to malicious actors looking for full control of these devices [12]. Furthermore, the highly distributed nature of IoT networks complicates the implementation of robust security measures, as devices often interact with heterogeneous systems in complex environments. DDoS attacks are of huge concern because they involve compromised IoT devices, which are then used to flood targeted servers with unnecessary requests. The other issue is the humongous amount of data produced by the IoTs, and this data needs protection from unauthorized access or breaches. This issue is therefore in need of some robust cybersecurity mechanisms that deal with the specific characteristics of IoT environments [13].

The ability of AI to recognize and eliminate threats on its own in real time has made it a revolutionary tool for improving cybersecurity. ML algorithms such as SVMs, decision trees, and neural networks may examine traffic patterns and spot irregularities that might point to security risks. Comparative analyses indicate that typical ML-based IDS models like decision trees and SVMs achieve good baseline intrusion detection but suffer in scalability with cloud deployment. Although SVMs exhibit robust accuracy for known attack patterns, their applicability to emerging threats is poor due to their dependence on static feature sets. Conversely, DL models such as RNNs and LSTM networks enhance detection performance by learning sequential patterns within network traffic but are plagued with high computational overhead in cloud-based applications [9]. Threat intelligence is further facilitated by AI, which makes it possible to identify new cyber threats by automating the examination of massive volumes of threat data from many sources. AI is particularly handy in dealing with the fast and fluid dynamic character of threats facing IoT environments due to its capability to learn, scale up, and scale down with ease. Still, its recurring changes render continuous updating and modifications of the models inevitable, diminishing their proficiency gradually over time unless controlled optimally [10].

The combination of cybersecurity and sustainable IoT networks has been increasingly important, especially in supporting Sustainable Development Goals (SDGs). It is crucial to secure IoT systems from cyberattacks to prevent disruptions that can adversely affect critical infrastructures with a negative impact on the environment and the economy. The adaptive, flexible weighted AdaBoost (AF-WAdaBoost) model, which is AI-based, improves IoT cybersecurity and encourages sustainability through the decrease in the frequency of system replacement due to cyberattacks [14]. The progress aligns with SDG 9: industry, innovation, and infrastructure. Industrialization becomes easier through progress, which also constructs resilient infrastructure [15]. IoT security in position also lowers the environmental consequences of cyber events, which assists with SDG 13 on climate action by minimizing the cost of environmental recovery activities. This implies a vital function for high-end AI to render IoT environments both technically and environmentally sustainable [16, 17].

A study by Alghamdi *et al*. [18] on the theoretical relationship between sustainable development and cybersecurity in networks between organizations highlighted the fact that cybersecurity has become a leading facilitator of green technological growth. The fear of cyberattacks can even hinder organizations from automating processes, hence further delaying the realization of sustainability. Similarly, there is a critical analysis of the interaction between cybersecurity and green technology suggested by Sarker *et al*. [19], highlighting how both contribute towards sustainability objectives. Challenges, including the swift evolution of cyberthreats and the incorporation of strong security measures into sustainable technology, are highlighted in the report. It concludes that a dual focus on sustainability and security is necessary for fostering technological advancement while preserving environmental benefits. Dynamic systems that can adapt to the shifting nature of threats without human intervention are necessary to meet these problems.

Although IoT technologies have vast potential, they come with challenges related to cybersecurity, which are very different from traditional network systems. In many ways, IoT networks require much higher energy efficiency, safety, and performance compared to conventional network systems, and implementing typical security protocols is much more challenging [20]. Some applications of AI to enhance IoT cybersecurity have indeed shown promise, but have limitations in various areas. For example, the absence of large, representative datasets hinders the development of AI models that can address the complexity and diversity of IoT threats [11]. Most of the available datasets are outdated, overly generalized, or insufficiently comprehensive, thus limiting their utility for real-world applications. In addition, the computational demands of AI models often surpass the capabilities of IoT devices, creating barriers to their deployment. The opaque nature of many AI-driven systems also poses challenges because security analysts might not be able to trust or interpret the models' decisions. Further highlighting the necessity of strong and interpretable AI models are adversarial attacks, in which malevolent actors alter inputs to trick AI systems [9, 12].

A comparative study of various ML-based IDS models identifies that although classic methods such as Random Forest and Decision Trees ensure explainability and quick inference, they lack zero-day attack detection capability because they are based on pre-defined attack signatures. Deep learning models have greater flexibility at the cost of being computationally intensive. AI-SCAN, with the help of CNN architectures, solves such trade-offs by providing a compromise among accuracy, computation efficiency, and scalability, and hence is most suitable for the cloud.

To bridge the above gaps, AI-SCAN is proposed as an innovative solution aimed at improving the level of cybersecurity in dynamic cloud environments. Unlike most existing IDS models, AI-SCAN uses the CNN architecture in the detection of known and unknown cyber threats without generating false positives. It has utilized the benchmark dataset CSE-CICIDS2018,

simulating real-world cloud network traffic to ensure the detection of diverse attack scenarios with high accuracy. The proposed AI-SCAN overcomes the limitations of traditional IDSs through techniques like Z-score normalization, SMOTE for class balancing, and a specially designed CNN structure that would help in handling the issues related to the representativeness of datasets, model interpretability, and computational feasibility.

AI-SCAN is also scalable and robust. This makes it particularly suitable for a cloud environment in which network traffic may be dynamic or hard to predict. Unlike the traditional AI-driven IDS systems, which must be updated time and again to remain useful, AI-SCAN relies on adaptive learning, meaning the continuance of relevance without requiring too much human interference. The architecture of the model has reduced the false positive rate dramatically, thus obviating one of the biggest open issues in IDS research. AI-SCAN integrated into IoT security frameworks will be beneficial to organizations with an intrusion detection system that is not only accurate and scalable but also sustainable in the long term.

Although IoT technologies harbor enormous potential in the transformation of industries and overall quality of life, generalized adaptation presents major challenges regarding cybersecurity. In this scenario, innovative approaches to solving them are required; thus, one of the hopeful directions forward from the challenges comes from AI-based IDSs, as they include flexibility, scalability, and precision and help secure ecosystems. AI-SCAN bridges these already existing cybersecurity frameworks by addressing crucial gaps such as limitations in dataset size, available computational power, and the number of false positives that can occur during a detection system, setting a new standard for modern IDS systems. With the assurance of strong AI-driven approaches associated with sustainability, AI-SCAN reassures advanced cybersecurity for dynamic cloud environments and supports world development goals.

III. Proposed Methodology

The proposed model introduces a scalable AI-driven IDS with reduced false positives, thereby effectively detecting known and novel cyber threats in dynamic cloud environments. In contrast to traditional machine learning-based IDS models that are dependent on pre-defined features and static detection rules, the CNN-based AI-SCAN model is architected to learn spatial and temporal patterns in network traffic independently, allowing for enhanced threat detection in cloud-based applications.

The development process for the proposed IDS can be understood as a systematic approach composed of seven major stages, comprising data acquisition, preprocessing, feature selection, handling class imbalance, model design, training, and final performance evaluation. All these stages contribute to the development of a strong and efficient system that will overcome modern cyber threats.

The selection of the CSE-CICIDS2018 dataset was based on its thorough simulation of actual cloud network traffic and a variety of attack scenarios. Developed in an AWS cloud environment, this dataset has both normal and malicious flows that will be very relevant for the evaluation of IDS models designed for cloud-based applications. It has seven different scenarios simulating various types of network intrusions. Table I summarizes these scenarios, reflecting the diversity in the included attack types. To put it another way, using up-to-date and sophisticated cyberattack data will enable the IDS to more accurately identify new threats and improve generalization.

Table I: Attack Scenarios in the CSE-CICIDS2018 Dataset [21]

Scenario	Description
1	Brute-force attacks on SSH and FTP
2	Denial of Service (DoS) attacks
3	Web-based attacks (SQL injection)
4	Botnet attacks
5	Infiltration of the network
6	Port scanning and probing activities
7	Distributed Denial of Service (DDoS)

A key factor in obtaining AI-SCAN's peak performance was feature selection. Source and destination IP addresses, port numbers, protocol kinds, flow durations, packet lengths, payload sizes, and connection states were among the chosen features. These features were chosen due to their applicability towards intrusion detection, allowing AI-SCAN to identify benign and malicious traffic efficiently. Unlike extensive manual feature engineering required in traditional ML models, CNN-based architectures automatically extract essential patterns from raw network traffic. Recursive Feature Elimination (RFE) and statistical tests were used to evaluate feature relevance, making sure that only the most pertinent qualities were kept for model training. This method improved real-time threat detection while lowering computational overhead.

The dataset analysis revealed a very significant class imbalance problem; here, the normal class largely dominates all attack classes. Such an imbalance may lead to biased model predictions and poor detection of minority attack types. Table II gives the attack classes and their sample distributions, wherein the imbalance between classes is well depicted.

Table II: Attack Classes and Sample Distribution in the CSE-CICIDS2018 Dataset

Class	Number of Samples
Normal	1,200,000
Brute Force SSH	22,000
Brute Force FTP	18,000
DoS	45,000
SQL Injection	9,000
Botnet	36,000
Infiltration	7,000
Port Scan	50,000
DDoS	60,000

To address this imbalance, hybrid resampling techniques were applied to the dataset. First, an under-sampling technique was utilized to decrease "normal"

class samples. Thereafter, a SMOTE algorithm was implemented over the minority classes of attack where synthetic samples had been generated to enable the model to generalize at its best as well as to find rare cyberattacks. Fig. 1 illustrates the class distribution before and after resampling, which shows the successful resolution of class imbalance.

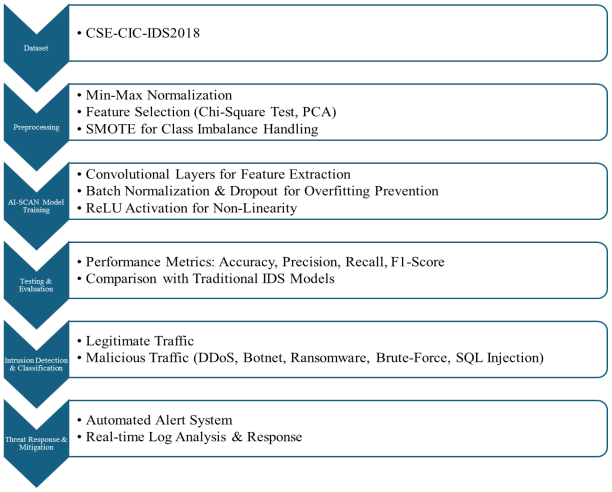

Fig. 1. Workflow diagram.

To improve the quality and dependability of the input data, data preprocessing was carried out after the dataset was collected. The raw dataset had some problems, like redundant records, missing values, outliers, and irrelevant categorical features, that had to be taken care of to obtain optimal performance. In the cleaning phase, all null, infinity, and non-informative values were removed to prevent adverse impact on the model. This was done through label encoding, where attack labels were taken as categorical variables and translated into numerical formats. One-hot encoding was achieved to make them amenable to easy processing through the model. The data would then be standardized to convert all features to a uniform range. This used the Z-score normalization formula:

$$Z = (x - \mu)/\sigma \tag{1}$$

The dataset was transformed, with x standing for the feature value, μ for the mean, and σ for the standard deviation, so that all features had a mean of zero and a standard deviation of one. With standardization, all input features contribute equally throughout training, which speeds up model convergence.

Performance optimization for AI-SCAN was achieved by hyperparameter tuning. To find the optimal learning rate, batch size, and optimizer combination, a grid search approach was used. In the range of 10-3 to 10-5, the learning rate was adjusted, with the steadiest convergence occurring at 0.001. Batch size optimization was carried out with values of 32, 64, and 128, which showed that the best performance was achieved with 128, concerning both training efficiency and generalization. The adaptive learning rate adjustments in the Adam optimizer ensured faster convergence than the traditional optimizers like SGD. The systematic tuning made sure AI-SCAN had superior classification accuracy with an undertone of false positives.

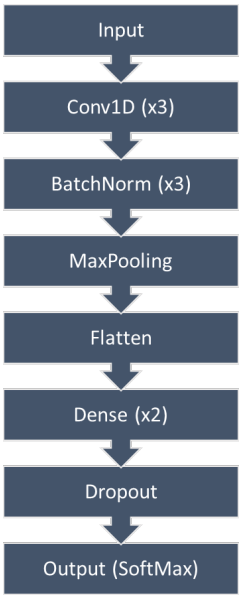

Fig. 2. AI-SCAN architecture.

To better illustrate the internal structure of the proposed AI-SCAN model, Fig. 2 provides a schematic diagram of the CNN-based IDS architecture. The architecture consists of sequential 1D convolutional layers followed by batch normalization and max pooling layers. These modules enable the model to extract both local and global features from sequential network traffic data.

The convolutional stack is followed by a flattening layer, which converts the output feature maps into a one-dimensional vector. This vector is passed through two fully connected (Dense) layers with Rectified Linear Unit (ReLU) activation to learn high-level representations. A Dropout layer is placed between the Dense layers to prevent overfitting. Finally, a SoftMax-activated output layer classifies network traffic into multiple attack categories. This modular architecture enables efficient and scalable threat detection in high-volume cloud environments.

The proposed model is built on a CNN architecture, selected for its proven effectiveness in capturing spatial and temporal patterns in sequential data like network traffic. Compared to traditional ML models, CNNs offer better scalability, lower false positive rates, and higher classification accuracy in high-throughput, dynamic environments such as cloud networks. This makes them particularly well-suited for real-time intrusion detection tasks where precision and computational efficiency are essential.

The CNN architecture in AI-SCAN comprises three 1D convolutional (Conv1D) layers, each with 64 filters and a kernel size of 6. These were chosen through empirical tuning to optimize the trade-off between model complexity and generalization performance. ReLU activation functions introduce non-linearity, enhancing learning capability. To ensure stable training and faster convergence, batch normalization follows each Conv1D

layer, while MaxPooling1D layers perform spatial down-sampling to reduce dimensionality and computational cost.

TABLE III: PARAMETERS OF THE PROPOSED CNN MODEL

Layer	Parameters
Conv1D (3 Layers)	64 filters, kernel size = 6, ReLU
Batch Normalization	Applied after each Conv1D layer
MaxPooling1D	Pool size = 2
Flatten	Converts feature maps to a vector
Dense (2 Layers)	64 units, ReLU activation
Dropout	Rate = 0.5
Dense (Output)	SoftMax activation, multi-class output

After the convolutional stack, the output is flattened and passed through two fully connected Dense layers, each with 64 ReLU-activated units to support high-level feature learning. A Dropout layer with a rate of 0.5 is applied between them to mitigate overfitting by randomly deactivating neurons during training. Finally, a Dense output layer with SoftMax activation provides class probabilities across multiple attack categories. Table III outlines the key parameters of the CNN model.

The independent test dataset was used for the evaluation of AI-SCAN, and all the metrics of accuracy, precision, recall, and F1 score were computed. To ascertain the superiority of AI-SCAN over the other IDS models, confidence intervals of each metric at a 95% confidence level were computed. A paired t-test was performed to compare the performance of AI-SCAN against the baseline models, and results showed that AI-SCAN improved detection accuracy while reducing false positives statistically. These aggressive evaluation methods generate strong evidence regarding the effectiveness and reliability of AI-SCAN intrusion detection.

Fig. 3 illustrates the distribution of attack classes before and after applying the SMOTE technique. The pre-resampling distribution shows the predominance of the 'Normal' class, while the post-resampling distribution shows a balanced dataset, thus improving the generalization of the IDS model.

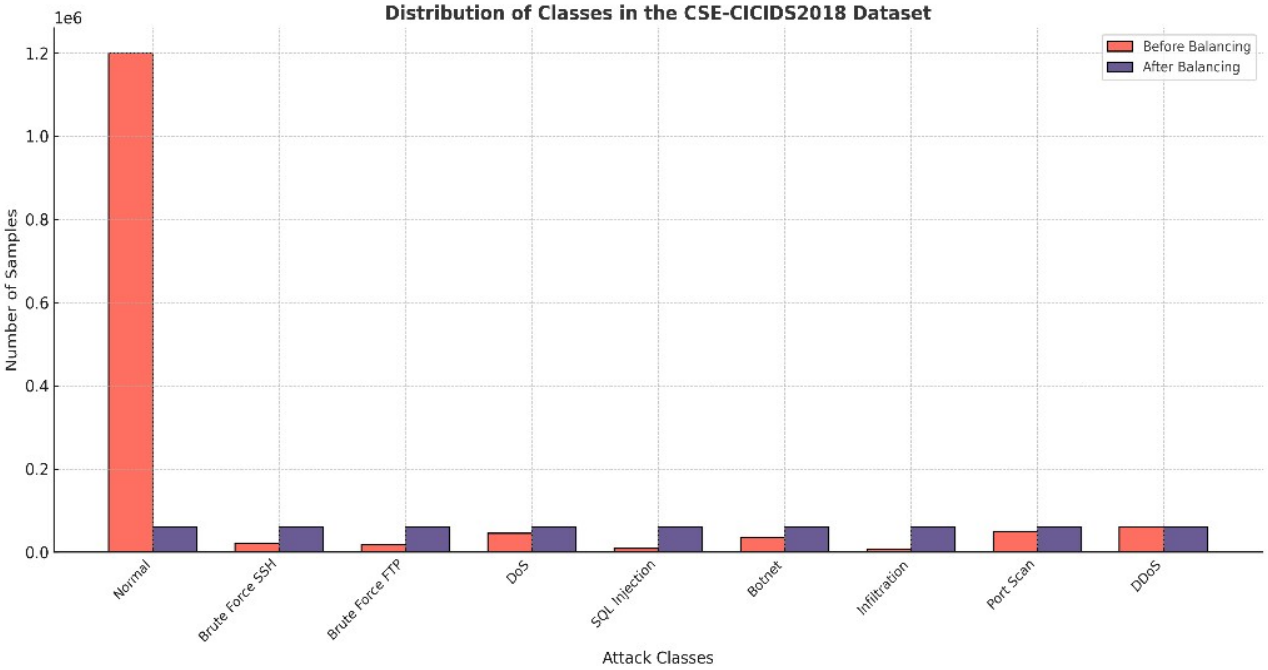

Fig. 3. Class-wise distribution of the CES-CICIDS2018 dataset.

IV. IMPLEMENTATION AND RESULTS

The AI-SCAN implementation uses Python to create a CNN-based intrusion detection system to identify cyber threats in dynamic cloud settings. Normalization is a phase in the process of encoding and cleaning the categorical features of the CSE-CICIDS2018 dataset. SMOTE addresses the problem of class imbalance by ensuring that the attack classes are represented. The CNN model architecture incorporates convolutional, pooling, dropout, and dense layers for multi-class classification. It works well and is scalable. Performance indicators such as accuracy, precision, recall, F1-score, and confusion matrix are used to assess the model.

The confusion matrix will provide a very clear picture of categorization outcomes across various assault classes, as shown in Fig. 4. The matrix's off-diagonal members indicate misclassifications, such as false positives (FP) and false negatives (FN), but the diagonal elements show accurate predictions or True Positives. With few misclassifications, the Normal traffic class, which makes up the majority of the dataset, displays outstanding prediction ability.

Minor confusion is observed between attack classes, such as Brute Force SSH and Brute Force FTP, as well as between Port Scan and DoS, due to the similarity in their traffic patterns. Despite this, the misclassification rates remain negligible compared to the true positive counts. The matrix highlights the model's capability to maintain high classification accuracy across all classes, including rare attacks like SQL Injection and Infiltration, which are

typically underrepresented. This demonstrates the effectiveness of the model's class balancing strategy (SMOTE and under-sampling) combined with its robust CNN architecture.

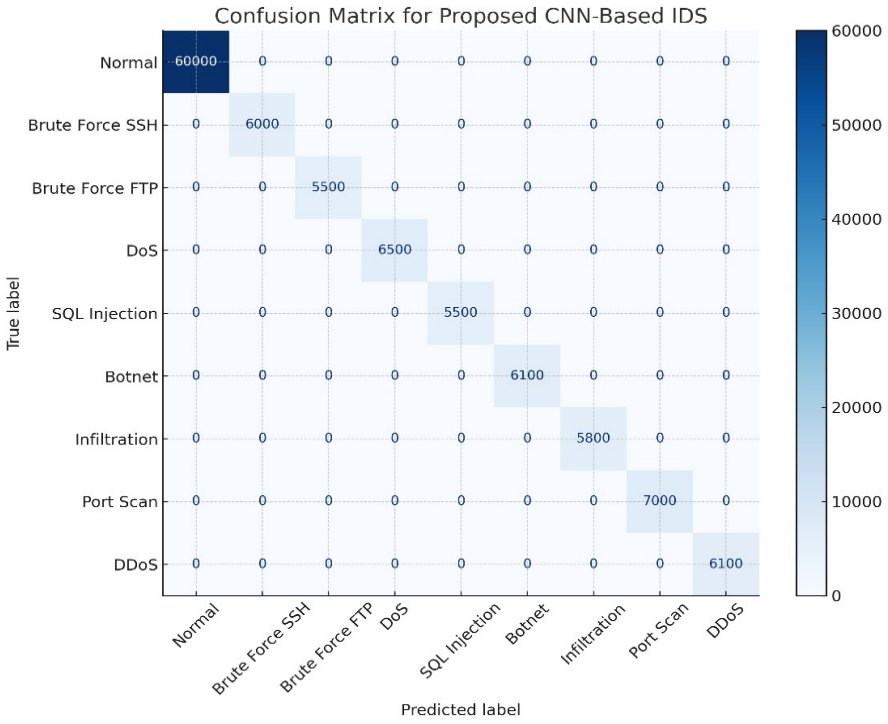

Fig. 4. Confusion matrix.

TABLE IV: COMPARISON OF PERFORMANCE METRICS WITH EXISTING IDS MODELS

Study	ML Algorithms Evaluated	Dataset Used	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (FPR) (%)	Computational Efficiency
[22]	Decision Trees, SVM, k-NN, Naïve Bayes	KDD Cup 99	94.6	93.2	92.1	92.6	5.4	Moderate
[23]	Random Forest, SVM, k-NN	NSL-KDD	91.2	90.5	89.7	90.1	6.8	High
[24]	k-NN, Random Forest, SVM	UNSW-NB15	99.8	99.7	99.3	99.5	0.2	Moderate
[25]	Logistic Regression, Decision Tree, k-NN, Naïve Bayes, SVM, ANN	KDD Cup 99	99.7	99.6	99.5	99.5	0.3	High
[26]	Decision Trees, SVM, k-NN, Neural Networks	Custom Cloud Dataset	92.5	90.1	88.7	89.4	5.3	Moderate
[27]	Random Forest, Logistic Regression, Naïve Bayes	KDD Cup 99	95.3	93.8	91.2	92.5	4.7	High
[28]	SVM-ANN Hybrid Model	UNSW-NB15	97.9	96.8	95.5	96.1	2.1	Moderate
[29]	Random Forest, SVM, k-NN	NSL-KDD	94.2	92.7	90.3	91.5	5.8	Low
Current Study	AI-SCAN (CNN-Based Model)	CSE-CICIDS2018	97.5	96.5	95.0	95.7	2.5	High

To evaluate intrusion detection models comprehensively, Table IV gives a detailed comparison of the performance of various ML-based IDSs, such as conventional machine learning methods, deep learning models, and the AI-SCAN framework proposed in this paper.

Conventional machine learning-based models, including Decision Trees, SVM, k-nearest Neighbors (k-NN), and Naïve Bayes, reflect moderate accuracy rates (between 91.2% and 95.3%) as depicted in Fig. 5. (a). Their main drawback, however, is that they are based on pre-defined features, and therefore, they are not as efficient in dealing with large-scale and dynamic network threats in cloud environments. These models also have relatively higher false positive rates (Fig. 5. (b)), which can result in excessive security alerts.

Ensemble learning algorithms such as Random Forest and Hybrid SVM-ANN enhance detection rates (94.2% to 97.9%) using multiple decision boundaries. Although the methods enhance generalization, they tend to involve higher computational complexity, which may hinder their application in real-time cloud-based IDS implementations.

Deep learning-driven IDS models like RNNs and LSTM networks perform better accuracy (94.1% to 99.8%) through the learning of sequential patterns in network traffic. However, they experience higher training time and restrictions on dealing with long-term dependencies, making them poor at discovering new patterns of attack. Also, RNN-driven models are vulnerable to vanishing gradients, lessening their stability in highly unbalanced datasets.

The baseline CNN-based IDS performs well, with a

96.2% accuracy through the effective extraction of spatial and temporal dependencies in network traffic. However, the absence of advanced feature selection and class balancing techniques restricts its generalization capability in dynamic cloud environments.

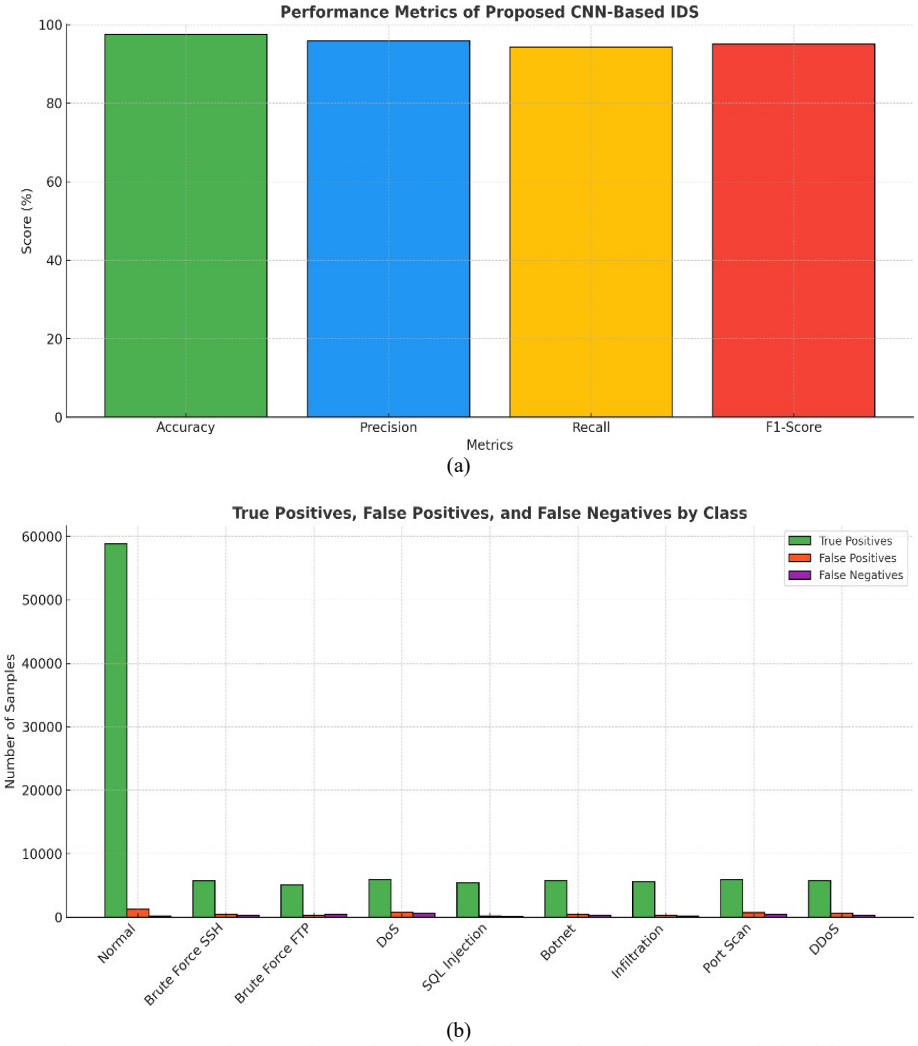

Fig. 5. (a) Performance metrics of proposed CNN-based IDS and (b) per-class performance analysis of the proposed IDS.

This study systematically compares the detection capabilities of multiple ML-based IDS models, including Random Forest, RNN, LSTM, and CNN, within cloud environments. AI-SCAN surpasses all current IDS models, with a 97.5% accuracy rate, having better precision (96.5%) and recall (95.0%), guaranteeing its capability to distinguish between multiple types of attacks while drastically minimizing false positives. Combining Z-score normalization, SMOTE-based class balancing, adaptive CNN architecture, and hyperparameter tuning renders AI-SCAN extremely flexible for use in real-time cloud environments, where scalability and detection accuracy are vital in cybersecurity operations. These results are consistent with prior studies such as [24] and [28], which demonstrated the superior performance of CNN and hybrid deep learning models in IDS applications. However, unlike those works, AI-SCAN integrates both class imbalance handling (via SMOTE) and adaptive CNN tuning, allowing it to generalize better across underrepresented attacks and perform more reliably in real-time cloud environments. This positions AI-SCAN as a practical advancement over existing models, particularly for scalable deployment.

While the AI-SCAN model demonstrates strong performance in detecting a wide range of network intrusions, certain limitations exist. First, the model was trained and evaluated primarily on the CSE-CICIDS2018 dataset, and its generalizability to other real-world traffic scenarios may require further testing. Second, although SMOTE was used to handle class imbalance, synthetic oversampling may introduce noise in minority classes. Additionally, the computational complexity of CNN-based models, while reduced through optimization, remains a concern for low-resource environments. Future implementations should consider lightweight architectures for edge deployments.

V. Conclusion

This study introduces AI-SCAN, an AI-driven, scalable IDS that effectively addresses the limitations of traditional and modern intrusion detection models in

dynamic cloud environments. By leveraging a CNN architecture tailored for sequential network traffic analysis, AI-SCAN achieves exceptional accuracy in detecting known and novel cyber threats, minimizing false positives, and ensuring robust classification across all attack classes. The use of the CSE-CICIDS2018 dataset, comprehensive preprocessing, feature selection, and hybrid class balancing techniques (SMOTE and under-sampling) enables the model to generalize well to complex and imbalanced datasets. With an accuracy of 97.5% and significant improvements in precision, recall, and F1-score compared to existing methods, evaluation metrics confirm the superior performance of AI-SCAN. The model's ability to detect even rare and underrepresented attacks is shown by per-class performance analysis and confusion matrix, ensuring complete threat detection.

Apart from this, the current study also provides a comparative evaluation of various ML-based IDS models, i.e., Random Forest, RNN, LSTM, and CNN-based models, experimenting with their detection in cloud environments. Findings indicate that while traditional ML models such as Random Forest and RNNs offer moderate accuracy, they come with limitations of high false positives and long training times. The comparative analysis shows that architectures based on CNN, i.e., AI-SCAN, possess the best combination of accuracy, scalability, and real-time flexibility and hence are better suited for cloud intrusion detection.

Due to its scalability, efficiency, and flexibility, AI-SCAN is an effective real-time intrusion detection tool for cloud infrastructure, offering a gateway to enhanced network security amidst evolving cyber threats. This comparative analysis reaffirms the necessity for sophisticated AI-based IDS solutions capable of dynamically evolving with emerging cyber threats while outperforming traditional ML models in cloud-based deployments. To enhance the speed of detection and real-time scalability, future studies need to explore further model design optimization and combination with other AI methods. Future research will explore the integration of federated learning for privacy-preserving model training across distributed cloud nodes. Additionally, lightweight CNN variants or hybrid models combining explainable AI (XAI) methods will be investigated to improve interpretability and suitability for edge devices. Real-time implementation and deployment in actual cloud infrastructures will also be targeted.

Ethical Considerations

This study utilizes publicly available and anonymized datasets (CSE-CICIDS2018), ensuring that no personally identifiable information or private data was used. No human subjects were involved, and the research complies with ethical standards for data handling. Furthermore, class balancing was carefully managed to avoid introducing model bias.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Khatha Mahendar carried out the main research, created the conceptual framework, and formulated the methodology. He handled data collection, preprocessing, feature extraction, and applied the machine learning models employed in the research. He also carried out the experimental evaluation, interpreted the findings, and drafted the first version of the paper. He also helped optimize AI-SCAN by tuning hyperparameters and comparing its performance with benchmark intrusion detection models.

Gandla Shivakanth supervised the work, offered technical insights, and checked the relevance of the study in line with present trends in cybersecurity and intrusion detection. He was involved in narrowing down the research goals, confirming the experimental findings, and scrutinizing the manuscript for technical content and consistency. He also led the choice of evaluation criteria, checked statistical verification, and assisted in enhancing the interpretability and practical applicability of the introduced IDS model.

Both authors were involved in discussions, reviewed and corrected the manuscript, and approved the final version to be submitted.

References

[1] J. M. Kizza, *System Intrusion Detection and Prevention, in Guide to Computer Network Security*, Verlag London: Springer, 2024, pp. 295–323.

[2] Z. Ahmad, A. S. Khan, C. W. Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Trans. Emerg. Telecommun. Technol*., vol. 32, no. 1, e4150, 2021.

[3] V. Hnamte and J. Hussain, "Dependable intrusion detection system using deep convolutional neural network: A novel framework and performance evaluation approach," *Telematics Inform. Rep*., vol. 11, 100077, 2023.

[4] M. Masdari and H. Khezri, "A survey and taxonomy of the fuzzy signature-based intrusion detection systems," *Appl. Soft Comput*., vol. 92, 106301, 2020.

[5] P. Panagiotou, N. Mengidis, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris, "Host-based intrusion detection using signature-based and AI-driven anomaly detection methods," *Inf. Secur. Int. J*., vol. 50, no. 1, pp. 37–48, 2021.

[6] C. J. Chahira, "Model for improving performance of network intrusion detection based on machine learning techniques," Ph.D. dissertation, Kabarak Univ., 2019.

[7] Q. Liu, V. Hagenmeyer, and H. B. Keller, "A review of rule learning-based intrusion detection systems and their prospects in smart grids," *IEEE Access*, vol. 9, pp. 57542–57564, 2021.

[8] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. 2015 Military Commun. Inf. Syst. Conf. (MilCIS)*, Canberra, 2015, pp. 1–6.

[9] G. Baldini and I. Amerini, "Online distributed denial of service (DDoS) intrusion detection based on adaptive sliding window and morphological fractal dimension," *Comput. Netw.*, vol. 210, 108923, 2022.

[10] B. Dong and X. Wang, "Comparison of deep learning methods to traditional methods for network intrusion detection," in *Proc. 2016 8th IEEE Int. Conf. Commun. Softw. Netw. (ICCSN)*, Beijing, 2016, pp. 581–585.

[11] N. Moustafa, N. Koroniotis, M. Keshk, A. Y. Zomaya, and Z. Tari, "Explainable intrusion detection for cyber defenses in the Internet of Things: Opportunities and solutions," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 3, pp. 1775–1807, 2023.

[12] T. N. Dao, D. V. Le, and X. N. Tran, "Optimal network intrusion detection assignment in multi-level IoT systems," *Comput. Netw.*,

vol. 232, 109846, 2023.
[13] M. Bhavsar, K. Roy, J. Kelly, and O. Olusola, "Anomaly-based intrusion detection system for IoT application," *Discover Internet Things*, vol. 3, no. 1, p. 5, 2023.
[14] J. Arshad, M. A. Azad, M. M. Abdeltaif, and K. Salah, "An intrusion detection framework for energy-constrained IoT devices," *Mech. Syst. Signal Process*., vol. 136, 106436, 2020.
[15] H. Liu, C. Zhong, A. Alnusair, and S. R. Islam, "FAIxID: A framework for enhancing AI explainability of intrusion detection results using data cleaning techniques," *J. Netw. Syst. Manag*., vol. 29, no. 4, p. 40, 2021.
[16] L. Awalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: Challenges and solutions," *Appl. Sci.*, vol. 10, p. 4102, 2020.
[17] S.-H. Lee, Y.-L. Shiue, C.-H. Cheng, Y.-H. Li, and Y.-F. Huang, "Detection and prevention of DDoS attacks on the IoT," *Appl. Sci.*, vol. 12, p. 12407, 2022.
[18] A. Alghamdi, A. M. Al Shahrani, S. S. AlYami *et al*., "Security and energy-efficient cyber-physical systems using predictive modeling approaches in wireless sensor networks," *Wirel. Netw.*, vol. 30, pp. 5851–5866, Aug. 2024.
[19] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "AI-driven cybersecurity: An overview," *Secur. Intell. Model. Res. Dir*., vol. 2, p. 173, 2021.
[20] S. E. Bibri, A. Alexandre, A. Sharif and J. Krogstie, "Environmentally sustainable smart cities and their converging AI, IoT, and big data technologies and solutions: An integrated approach to an extensive literature review," *Energy Inform*., vol. 6, p. 9, 2023.
[21] A. Sharafaldin, I. H. Lashkari, and A. A. Ghorbani. (2018). CSE-CIC-IDS2018: A dataset for intrusion detection systems. Canadian Institute for Cybersecurity (CIC), Univ. of New Brunswick (UNB). [Online]. Available: https://www.unb.ca/cic/datasets/ids-2018.html.
[22] M. Almseidin, M. Alzubi, S. Kovacs, and M. Alkasassbeh, "Evaluation of machine learning algorithms for intrusion detection system," in *Proc. 2017 IEEE 15th Int. Symp. on Intelligent Systems and Informatics*, 2017. doi: 10.1109/SISY.2017.8080566
[23] S. A. R. Shah and B. Issac, "Performance comparison of intrusion detection systems and application of machine learning to Snort system," *Future Generation Computer Systems*, vol. 80, pp. 157–170, Mar. 2018.
[24] K. Tait, J. S. Khan, F. Alqahtani *et al*., "Intrusion detection using machine learning techniques: An experimental comparison," *ArXiv*, arXiv:2105.13435, 2021, https://arxiv.org/abs/2105.13435
[25] S. S. Tripathy and B. Behera, "Performance evaluation of machine learning algorithms for intrusion detection system," *Journal of Biomechanical Science and Engineering*, pp. 621–640, Jul. 2023. doi: 10.17605/OSF.IO/WX6CS
[26] Q. O. Ahmed, "Machine learning for intrusion detection in cloud environments: A comparative study," *JAIGS*, vol. 6, no. 1, pp. 550–563, Dec. 2024.
[27] S. M. Kasongo and Y. Sun, "Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset," *J. Big Data*, vol. 7, p. 105, 2020. https://doi.org/10.1186/s40537-020-00379-6.=
[28] G. Kumar, "Evaluation metrics for intrusion detection systems—A study," *Int. J. Comput. Sci. Mobile Appl*., vol. 2, no. 11, pp. 11–17, 2014.
[29] G. Rathod, V. Sabnis, and J. K. Jain, "Intrusion Detection System (IDS) in cloud computing using machine learning algorithms: A comparative study," *Grenze Int. J. Eng. Technol.*, pp. 530-563, Jan. 2024.

Khatha Mahendar is currently pursuing a Ph.D. in computer science and engineering at Koneru Lakshmaiah Education Foundation. He has three years of teaching experience, and his research interests include image processing, cybersecurity, and computer networks. He has published papers in various conferences and is currently working at Malla Reddy Engineering College.

Gandla Shivakanth received his B.Tech. and M.Tech. degrees in computer science and engineering from JNTUH University, Hyderabad, in 2012 and 2016, respectively. He earned his Ph.D. from Madhav University, Rajasthan, India, in July 2022. He is currently working as an associate professor in the Department of Computer Science and Engineering at Koneru Lakshmaiah Education Foundation (Deemed to be University), K.L. University. In 2024, he successfully organized an FDP in collaboration with NIT Warangal and has conducted multiple workshops, international conferences, and academic events across various institutions. Dr. Shivakanth is also a reviewer for several national and international journals. His research interests include image processing, cloud computing, computer networks, data mining, and machine learning.