Journal of Global Research in Electronics and Communication (JGREC)
Volume 2 | Issue 11 | November 2026 | Pages 22–28
DOI: https://doi.org/xxxxxxxxxxxxx
e-ISSN: 2321-3175
Research Article OPEN ACCESS Available online: https://jgrec.info/index.php/jgrec/index

Machine Learning–Based Security Threat Detection in Cloud Computing Environments

Ms. Shivani Jain
Assistant Professor
Department of Computer Science and Applications
Mandsaur
shivani.jain@meu.edu.in

Corresponding Author: * Shivani Jain (shivani.jain@meu.edu.in)

Received: 10 November 2026 | **Revised:** 15 November 2026 | **Accepted:** 20 November, 2026

***Abstract*— Cloud computing's dynamism and multi-tenant nature make it vulnerable to complex cybersecurity threats, but it has also become an essential platform for distributed services and scalable data storage. The real-time detection of developing and zero-day assaults is often missed by traditional security systems. Using the NSL-KDD dataset, this paper suggests a threat detection methodology based on machine learning to improve cloud intrusion detection. The approach incorporates preprocessing methods, feature selection based on Random Forest, and two sophisticated models: XGBoost and a stacked ensemble that uses Logistic Regression as the meta-learner and combines Decision Tree, RF, and Gradient Boosting. These metrics—AUC-ROC, F1score, recall, accuracy, and precision—are used to assess performance. With an AUC of 1.0 and detection accuracies of up to 99%, the experimental results show that the model performs very well in classification tasks. The recommended strategy augments detection reliability, decreases misclassification, and delivers a scalable, data-informed way to fortify cloud security systems.**

Keywords*— *Cloud Computing Security, Machine Learning, Cyber Threat Detection, Cloud Network Security, Predictive Analytics.

I. INTRODUCTION

Software, networking, and data storage have all been revolutionized by cloud computing. They are hosted on remote servers and accessed online [1], [2]. This technology offers scalability, cost efficiency and accessibility, making it a popular choice for businesses and individuals [3], [4]. With many benefits, it comes with challenges, especially around security, and the Cybersecurity industry plays a crucial role in discovering and implementing solutions. Cloud is vulnerable to Malware, Viruses, Phishing, SQL injection, Cross-Site scripting, DoS Attack, Zero-Day, Botnet, Man-in-the-Middle and many more [5], [6], are used by cyber criminals to steal data and disrupt services to prevent such attacks Intrusion Detection and anomaly based detection plays a crucial role and as the advisories get smarter the Cybersecurity industry needs to in par in inventing better methods and security solutions to counter cybersecurity attacks [7], [8][9][10]. The dependability of services offered in different industries is greatly jeopardized by these dangers, which also endanger data integrity and privacy [11], [12]. Thus, enhancing security measures in cloud environments is of paramount importance [13], [14]. Traditional security mechanisms, which often involve static rule-based systems, are increasingly proving inadequate against sophisticated cyber-attacks that evolve at a rapid pace. Such methods are not only resource-intensive but also limited in their ability to adapt to new, previously unencountered threats. In response, there has been a significant shift towards leveraging Artificial Intelligence (AI) in cybersecurity [15]. AI-powered systems, with their ability to learn from data, offer a dynamic approach to security by enabling real-time threat detection and response [16], [17]. ML is a type of AI that improves threat detection by allowing computers to learn from previous data, discover complicated patterns, and adapt to new attack techniques [18]. These models can detect subtle behavioral deviations, predict potential vulnerabilities, and trigger real-time alerts. Techniques such as supervised learning, unsupervised anomaly detection, and clustering are commonly used to identify threats that would otherwise go unnoticed [19], [20]. ML greatly enhances the entire security posture by increasing detection accuracy, decreasing false positives, and supporting automated incident triage [21], [22]. AI and ML algorithms can process and analyze massive datasets in real time, enabling the detection of anomalies and emerging threats with greater speed and accuracy compared to traditional methods [23]. AI and ML can analyze enormous volumes of security-related data to identify patterns and anomalies indicative of potential threats.

A. Motivation and Contributions of the Study

The quick incorporation of cloud computing in several sectors has presented intricate security issues stemming from shared resources, virtualized environments, and perpetually advancing cyber threats. False alarms are common because traditional rule-based intrusion detection systems can't adjust to changing assault patterns. Because of this, there is a pressing demand for automated threat detection systems that can learn from massive amounts of network data. In order to safeguard contemporary cloud ecosystems, machine learning can detect concealed attack behaviors, allowing for proactive

Copyright © 2026 The Author(s).
This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) License (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, adaptation, and reproduction in any medium, provided the original author(s) and the source are properly credited.

J. Glob. Res. Elec. Comm., 2 (11):22-28
DOI: https://doi.org/xxxxxxxxxxxx

and precise defense. Key findings from the research are presented:

- Proposes a machine learning–driven framework for detecting cybersecurity threats in cloud environments.
- Implements comprehensive preprocessing, including encoding, normalization, and class balancing, to improve data quality.
- Applies Random Forest–based feature selection to reduce dimensionality and enhance computational efficiency.
- Develops a stacked ensemble model and XGBoost to compare robustness and predictive performance.
- Provides a scalable and adaptable solution suitable for real-time cloud security monitoring.

B. *Justification and Novelty of the Paper*

The growing requirement for cloud-specific threat detection technologies that are lightweight, accurate, and scalable justifies the research. A hybrid ensemble framework integrating feature-optimized learning, stacking generalization, and XGBoost is suggested in this study, in contrast to previous research that relies on single-model techniques or static detection mechanism. To increase detection accuracy, minimize false predictions, and promote generalization across varied cloud traffic patterns, the unique approach is to integrate ensemble intelligence with Random Forest-based feature selection.

C. *Structure of the Paper*

Here is the outline of the paper: Research gaps are identified and relevant literature is reviewed in Section II. The methodology and methods used to create the model are discussed in detail in Section III. The findings and comparisons of the investigations are detailed in Section IV. Finally, Section V concludes the analysis and outlines the research goals moving forward.

II. Literature Review

Recent research has focused on using ML and DL techniques to discover security risks in the cloud, with a focus on accuracy, scalability, anomaly detection, and real-time monitoring.

A. K. Shukla et al. (2026) propose the Shuffle Attention Convolutional ForwardFractionalNetwork (SACFFNet) to address weaknesses in cloud computing by detecting performance-compromising assaults. The SACFFNet model, which combines Fractional Calculus with Shuffle Attention Networks and Convolutional Neural Networks, achieves a sensitivity of 92.884% and a specificity of 92.090%, with an accuracy of 101.678 percent [24]. X. Jiang et al. (2025) provide a deep learning model that find abnormalities and threat early warning systems in cloud-based infrastructures in real-time using LSTM analysis and attention. The system's accuracy with the threat prediction is 96.8 percent, its rec rate is 95.7 percent, and its average lead time is 142 percent. Proving its scalability and business product efficiency, it has been implemented in three major cloud systems [25].

V. Mamidala et al. (2025) conducted a study to evaluate the efficacy of the Isolation Forest (I Forest) algorithm in detecting anomalies in cloud environments to protect data and information from cyber threats. The I Forest algorithm was more successful than traditional methods, scoring an average of 0.842 and a FNR of 0.06, at a fast processing time. The results indicate that I Forest can significantly enhance the accuracy of threat detection and can be easily integrated with the existing security infrastructures [26]. T. A. Devi and A. Jain (2024) introduced a new approach to intrusion detection in cloud computing based on deep-learning techniques. They emphasize the need to supplement training data to increase the detection effectiveness of offline and online training. Soft-max regression and STL are capable of learning features that result in a higher than 98% accuracy in various classification categories [27].

D. Chaudhary et al. (2024) suggests a cutting-edge AI-based strategy to improve cloud-based cyber threat identification and mitigation. The suggested approach attains 98.5% detection acc as opposed to the current system's 89.7%, while lowering the FN and FP rates to 2.0% and 1.2%, respectively [28]. P. Parameswarappa et al. (2023) provide a novel firewall approach that uses a ML algorithm to ensure cloud computing is secure. By merging previous node judgements with the ML algorithm's output on the publicly accessible UNSW-NB-15dataset, the suggested approaches predict the final attack category and enhance anomaly detection by 97.68% [29].

A. *Critical Gaps in Existing Research*

Although there have been significant improvements regarding ML-based security measures to cloud computing, a number of constraints remain. The existing methods are mostly focused on high levels of detection but do not consider real-time flexibility against the existing and zero-day attacks in dynamic cloud environments. Also, most models are based on static or benchmark datasets that fail to reflect the complexity of multi-tenant, large-scale cloud infrastructures, which prevents real-world usage. Computational cost, scalability, and resource-constrained cloud systems integration are issues that have not been sufficiently studied. Moreover, explainable, and lightweight frameworks that can guarantee efficient threat detection whilst still preserving privacy, interoperability, and ensuring continuous learning in heterogeneous cloud ecosystems cannot be explained.

III. Methodology

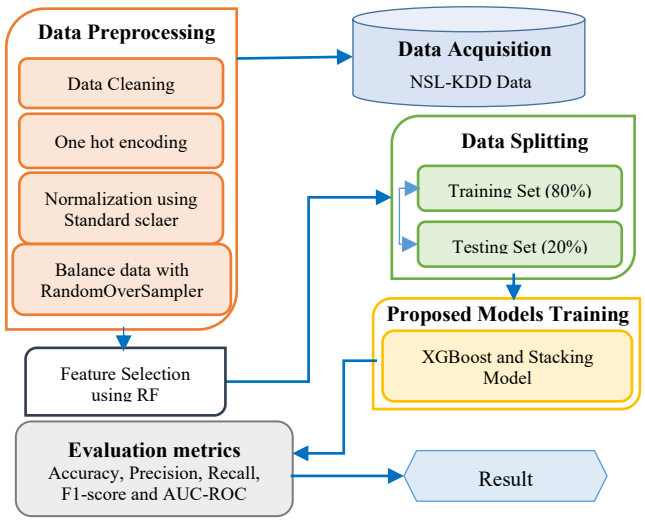

Fig. 1. Workflow of Machine Learning–Based Threat Detection in Cloud Networks.

The suggested approach for ML-based cloud security threat detection (Fig. 1) starts with data gathering from the NSL-KDD dataset, which includes intrusion logs and network

J. Glob. Res. Elec. Comm., 2 (11):22-28
DOI: https://doi.org/xxxxxxxxxxxxx

traffic. The raw data undergoes preprocessing, including data cleaning, one-hot encoding, normalization using a standard scaler, and balancing with Random Over Sampler to handle class imbalance. The most relevant characteristics are then found by feature selection utilizing an RF technique, increasing model efficiency. The processed data is divided into training (80%) and testing (20%) subsets. It suggests a combination of DT, RF, and GB or XGBoost as a threat detection model. To provide proper identification, studies use such measures as F1score, acc, prec, rec, and AUC-ROC to assess the performance of the models.

A. Data Collection

The NSL-KDD dataset [30] is utilized in this study as a refined version of the KDD Cup'99dataset, designed to overcome redundancy and class imbalance limitations. It comprises 41 characteristics such as categorical, binary, and continuous variables that manifest different network traffic patterns. The instances are also categorized as normal and attack with attack types being DoS, Probe, R2L and U2R. Due to its enhanced data distribution and less bias, NSL-KDD is highly apt in benchmarking intrusion detection system in cloud and network security studies.

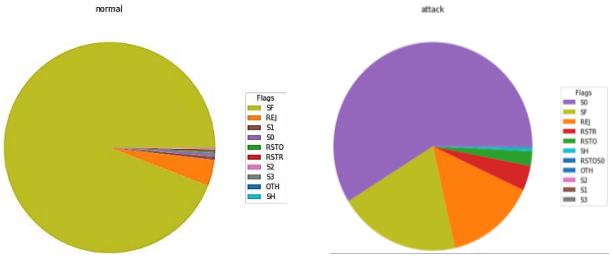

Fig. 2. Distribution of Connection Flags in Normal and Attack Network Traffic.

Fig. 2 provides the comparison between connection flag distributions of normal and attack traffic. Normal traffic is predominantly comprised of the SF flag, which is a successful connection, whereas the attack traffic includes a broader variety of flags including S0, REJ, and RSTR, which are an abnormal or failed connection attempt.

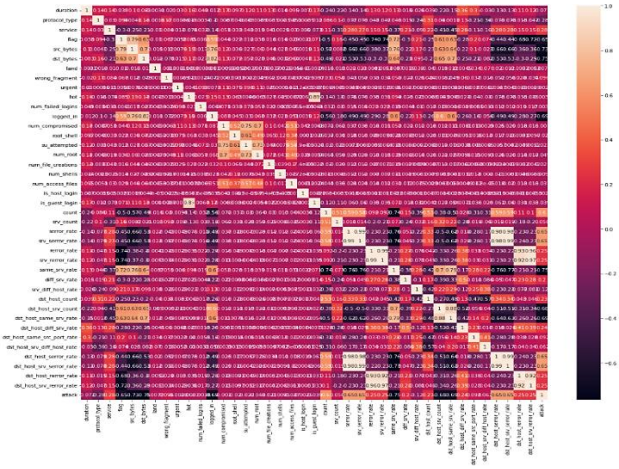

Fig. 3. Correlation Matrix of Network Traffic Features.

Fig. 3 displays a heatmap of the Correlation Matrix of the network traffic feature, with the color intensity indicating the magnitude and direction of the relationships between variables. Light colors denote positive correlations, whereas the dark colors present weak or negative associations.

B. Data Preprocessing

Data pre-processing is crucial to prepare data to be selected according to features because machine learning algorithms need numerical and clean data. The following steps are undertaken to achieve this:

1) Data Cleaning

Data cleaning is done to ensure the correctness and uniformity of the dataset prior to modelling training. The data are analyzed in terms of duplicate entries, null records, and formatting errors. The extra spaces and other unusual characters are then eliminated from the categorical data that has been categorized as protocol type, service, and flag. The step removes noise and provides reliable and structured data to model intrusion detection accurately.

2) Encoding

Encoding is carried out to encode categorical attributes in the data to numerical representations that can be processed with machine learning algorithms. The protocol type and service, as well as flag features, are coded as one-hot features [31]. This guarantees that the category information is maintained without violation of ordinal bias. The encoded data allows the classifiers to do processing on network traffic characteristics to make intrusion determination.

3) Normalization

The pre-processing method in machine learning is the Standard Scaler used to normalize dataset features to a mean of 0 and a standard deviation of 1 [32]. The average and standard deviation for every feature in the dataset are computed as Equation (1):

$$z = \frac{x-\mu}{\sigma} \quad (1)$$

Where z represents a normalized value, x is the original feature value, μ denotes the mean of the feature, and σ denotes its Standard Deviation.

4) Balance data with RandomOverSampler

RandomOverSampler to increase the number of instances of minority classes is used to counteract the imbalance between the classes in the NSL-KDD dataset. Fig. 4 indicates the Class Distribution of the data prior to and after balancing. Firstly, the data was skewed (67,343 normal and 58,630 attack), though, with the oversampling, the data were equalized (67,343 samples per classes), therefore, making both balanced when training the model.

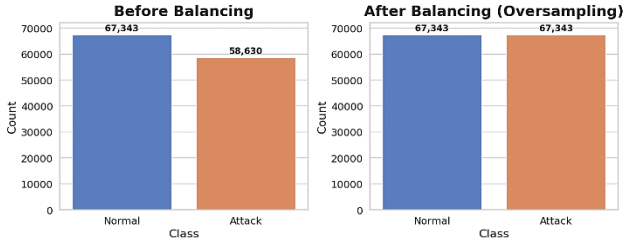

Fig. 4. Data Distribution Before vs After Balancing.

5) Feature Selection using RF

Random Forest feature selection defines the most important attributes with the help of feature importance scores, which are based on decision tree splits. Key selected features include src_bytes, data transfer, same_srv_rate, count, dst_bytes, dst_host_serror_rate, dst_host_diff_srv_rate, dst_host_srv_serror_rate,

J. Glob. Res. Elec. Comm., 2 (11):22-28
DOI: https://doi.org/xxxxxxxxxxxxx

srv_serror_rate, error rate, and attack. The more important features are kept and less significant ones are eliminated, resulting in dimensional reduction and enhancing the effectiveness and generalization of the model.

6) Data Splitting

In this analysis, each dataset is divided into two distinct parts at a ratio of 80:20. The majority, or 80%, of the data is utilized to train the model, with the remaining 20% set aside for performance assessment.

C. Implementation of ML Models

The proposed models are defined below, which are used for prediction the cloud security.

1) Stacking Model

The proposed method involves the stacking of ensemble model, which will combine DT, RF, and GB as base learners to improve classification strength and predictive power [33], [34]. The bottom level of the stacked architecture has individual base classifiers that are trained separately on the training data and thus are able to extract a variety of decision patterns and interactions between features. K-fold cross-validation is utilized to obtain out-of-fold prediction using each of the base models in order to obtain reliable performance and to reduce over-fitting.

These initial-level predictions are then put together to create a new space of features which are fed into a second-level meta-learner on LR. LR is a linear probabilistic classifier which is based on a sigmoid activation function in order to estimate the probability of a class and models the relation between the input variables and the target class. LR as a meta-learner determines the best weightings of the prediction of DT, RF, and GB, which is the degree of influence that each base model is supposed to contribute to the final decision. The strategy can be further enhanced by layering the models to achieve complementary strengths, reduce bias, and variance and enhance their overall generalization behavior over individual classifiers.

2) XGBoost Model

XGBoost is a superior ensemble learning algorithm founded on gradient boosting, in which the decision trees are built upon each other, and each subsequent tree is intended to eliminate the errors made by other trees [35]. XGBoost will enhance the capability of classification in the proposed intrusion detection model, by taking into account the complicated nonlinear relationship amid network traffic characteristics. Its residual-learning algorithm allows self-improvement allowing it to operate its accurate detection of normal and malicious processes which increases its detection accuracy and strength. The XGBoost problem is defined as illustrated in Equation (2).

$$\mathcal{L}(\emptyset) = \sum_{i=1}^{n} l(y_i, \hat{y}_i) + \sum_{k=1}^{K} \Omega(f_k) \quad (2)$$

Where $\mathcal{L}(\emptyset)$ represent the overall loss function, l is a differentiable convex loss function that measures the discrepancy among the forecast results $\hat{y}_i$ and the true value y_i , and Ω is the phrase used for regularization, which reduces the model's complexity.

In training it is a gradient-based optimization of this objective function which is reduced by the model with hyperparameters including Learning Rate, tree depth, and number of estimators being optimized to obtain the best possible generalization performance.

D. Evaluation Metrics

The effectiveness of the proposed plan can be measured with the help of the indicators offered in this section. TP, TN, FP, and FN were the fundamental elements of the evaluation [36]. Accuracy, or the proportion of accurate forecasts to all instances, is one of the primary performance metrics based on these figures. Precision is used to determine the accuracy of optimistic forecasts. Recall measures the ability of the model to locate all the relevant examples. F1score particularly can be used where there is imbalance in the classes since it considers both FP and FN. In order to depict the sensitivity and the FPR at different thresholds it will make the ROC curve. A greater number approaching 1 indicates strong performance when measuring the AUC, which is utilized to quantify the overall performance of the model. The Mathematical computation is shown in Equations (3) to (7).

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (3)$$

$$Precision = \frac{TP}{TP+FP} \quad (4)$$

$$Recall = \frac{TP}{TP+FN} \quad (5)$$

$$F1 = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (6)$$

$$AUC = \int_0^1 TPR(FPR)d(FPR) \quad (7)$$

Where FPR stands for false positive rate and TPR for true positive rate. This comprehensive assessment of the models' efficacy is achieved when these metrics are combined.

IV. Result Analysis and Discussion

The experiments were performed within the Windows-based system that provided a high-performance AMD Ryzen 9 processor and 64 GB RAM to provide efficient training and evaluation of various models. Table I shows comparative results between the two proposed models, Stacking and XGBoost, in the detection of security threats in Cloud Computing environments. Both models are highly predictive, virtually perfect on all evaluation criteria. Although both models achieve an AUC-ROC of 1.0, demonstrating outstanding classification effectiveness and reliability, Stacking model notably outperforms XGBoost in acc, prec, rec and F1score.

TABLE I. Performance Analysis of Proposed Ensemble Stacking and XGBoost Model

Metric	Stacking model	XGBoost model
Accuracy	99.0	98.79
Precision	99.2	98.78
Recall	99.7	99
F1-Score	99.45	98.89
AUC-ROC	1.0	1.0

The confusion matrices in Fig. 5 indicate that both the XGBoost and stacking ensemble model possess very high classification accuracy on 22 attack types and the normal category. The diagonal values (almost 276-279 correct predictions per class) are strong and almost zero-off-diagonal values show that there is little misclassification. This demonstrates the high accuracy of the models and their potential to successfully discriminate between various cyber threats.

DOI: https://doi.org/xxxxxxxxxxxxx

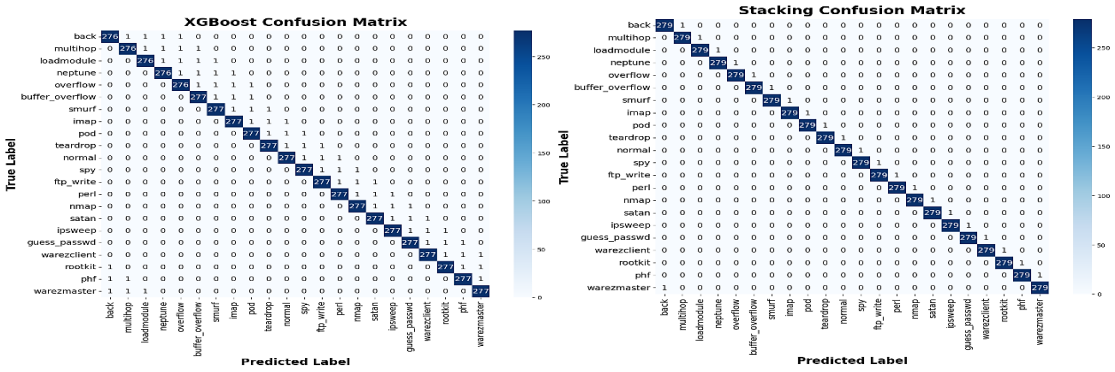

Fig. 5. Confusion Matrix of XGBoost Model for threat detection in the cloud.

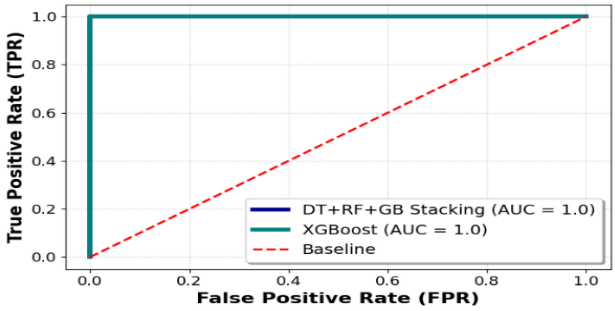

Fig. 6. ROC Curve of Stacking Ensemble and XGBoost Models.

Fig 6 shows the ROC curve illustrating that both the Stacking Ensemble and XGBoost models show an excellent performance with an AUC of 1.0. This implies that it is perfectly classified with a 100 percent true positive rate and zero false positives, which points to their efficiency in identifying various cybersecurity threats.

A. Comparative Analysis

Table II displays the results of comparing several ML models implemented on various intrusion detection datasets. The model with the highest performance is the proposed one based on the NSL-KDD dataset, the accuracy of the Stacking model is 99.0 percent, XGBoost is 98.79 percent, which is higher than past-reported models. Other works present lower accuracies, such as RF-RBFNN (94.16%) on NSL-KDD, KNN (98.21%) on SDN Data, ANN (92.0%) on ISOT-CID, and SVM (94.32%) on CICDDoS2019. In general, the results indicate that the ensemble-based method proposed achieves better detection rates than current methods.

TABLE II. COMPARATIVE PERFORMANCE ANALYSIS OF MACHINE LEARNING MODELS FOR CLOUD SECURITY

Reference	Dataset	Models	Accuracy
Proposed	NSL-KDD	Stacking model	99.0
Proposed	NSL-KDD	XGBoost	98.79
[37]	NSL-KDD	RF-RBFNN	94.16
[38]	SDN Data	KNN	98.21
[39]	ISOT-CID	ANN	92.0
[40]	CICDDoS2019	SVM	94.32

B. Discussion

The experimental results indicate that when the ability of numerous classifiers is combined, ensemble learning significantly enhances cloud-based cybersecurity threats detection. The stacking model, especially, demonstrated better performance because it is capable of incorporating different decision patterns and decreasing both bias and variance. The large AUC-ROC and low misclassification rates show great generalization ability to differentiate normal and malicious traffic. The proposed framework is more accurate than the current methods and offers better computational efficiency as a result of feature selection. Nevertheless, the controlled dataset environment might fail to capture dynamic attack patterns, and it is important to emphasize that real-time validation, as well as adaptive learning mechanisms, should be deployed in dynamic cloud infrastructure.

V. CONCLUSION AND FUTURE WORK

An ML-based system was developed to detect cybersecurity problems in cloud computing environments with advanced ensemble learning approaches. By combining extensive preprocessing, feature selection using the Random Forest algorithm, and having such a powerful classifier as XGBoost and a stacked ensemble model, the system was able to identify malicious activities with a high accuracy and reliability. The stacking model was better in all the measures of evaluation, showing the effectiveness of using a combination of multiple learners to learn the tricky and dynamic attack patterns. The results emphasize that highly intelligent data-driven detection mechanisms can go a long way to outshine the traditional intrusion detection methods in terms of enhancing anomaly recognition and minimizing false alarms. The proposed architecture is highly applicable in modern distributed cloud infrastructures because of its scalability and flexibility. Though the findings were promising, the test was mainly done with benchmark collections and this might not reflect the dynamic and heterogeneous nature of actual cloud environments. Future studies will focus on validation on live cloud traffic and large-scale, multi-tenant systems so that it can be practically applicable. The use of explainable artificial intelligence methods will also increase the transparency, interpretability, and user confidence in automated threat detection systems. Moreover, investigating lightweight and federated learning approaches will help conduct privacy-aware, real-time monitoring with reduced computational needs, allowing to perform threat detection safely and efficiently under different and resource-limited cloud systems.

- **Funding:** This research received no external funding.
- **Institutional Review Board Statement:** Not applicable.
- **Informed Consent Statement:** Not applicable.
- **Data Availability Statement:** The data supporting the findings of this study are available from the corresponding author upon reasonable request.
- **Conflicts of Interest:** The author declares no conflict of

How to cite this article:
S. Jain, "Machine Learning–Based Security Threat Detection in Cloud Computing Environments," *Journal of Global Research in Electronics and Communication*, vol. 2, no. 11, pp. 22–28, Nov. 2026, Doi: XXX

REFERENCES

[1] K. K. Mohammed, "The Future is Cloud : Modernizing Big Data for the Cloud Era," *Int. J. Sci. Res. Eng. Trends*, vol. 11, no. 5, pp. 1–5, 2025.

[2] S. Karri, C. M. Penugonda, S. Karanam, M. Tajammul, S. Rayankula, and P. Vankadara, "Enhancing Cloud-Native Applications: A Comparative Study of Java-To-Go Micro Services Migration," *Int. Trans. Electr. Eng. Comput. Sci.*, vol. 4, no. 1, pp. 1–12, Apr. 2025, doi: 10.62760/iteecs.4.1.2025.127.

[3] A. Warrier, "Securing and Scaling API Gateways in Hybrid Environments," *J. Artif. Intell. Mach. Learn. Data Sci.*, vol. 3, no. 3, pp. 2914–2920, Sep. 2025, doi: 10.51219/JAIMLD/Arjun-warrier/607.

[4] M. Parikh, A. A. Soni, S. M. Shah, and A. R. Jha, "Big Data Workload Profiling for Energy-Aware Cloud Resource Management," in *2026 International Conference on Data Analytics for Sustainability and Engineering Technology (DASET 2026)), Track: Big Data and Machine Learning Applications*, IEEE, Ed., arXiv preprint arXiv, 2026, pp. 01–07, januray. doi: 10.48550/arXiv.2601.11935.

[5] V. K. Sharma, "Cloud Computing \& IoT: 5G Focused IoT with Cloud Solutions," *Int. J. Artif. Intell. Big Data, Cloud Comput. Data Sci.*, vol. 6, no. 3, pp. 21–25, Jul. 2025.

[6] V. Varma, "Secure Cloud Computing with Machine Learning and Data Analytics for Business Optimization," *J. Eng. Technol. Adv.*, vol. 4, no. 3, pp. 181–188, 2024, doi: 10.56472/25832646/JETA-V4I3P119.

[7] R. V. S. S. B. R, Y. M. M. John, M. B. B. G, B. Karim, and G. Saritha, "Multi-Domain Cyber Threat Classification Using Enhanced Genetic Algorithm and Deep Neural Networks," in *2025 Third International Conference on Networks, Multimedia and Information Technology (NMITCON)*, IEEE, Aug. 2025, pp. 1–6. doi: 10.1109/NMITCON65824.2025.11187556.

[8] J. E. Kofi, "Monitoring Cloud Performance Metrics Utilizing AI to Estimate the Efficiency of Cloud Operations," in *2025 7th International Symposium on Advanced Electrical and Communication Technologies (ISAECT)*, IEEE, Dec. 2025, pp. 1–6. doi: 10.1109/ISAECT68904.2025.11318827.

[9] M. H. Hamza Afzal, "Securing AI Systems Against Adversarial Attacks: A Framework for Building Robust and Trustworthy Machine Learning Models," *Comput. Fraud Secur.*, vol. 2024, no. 5, pp. 65–74, May 2024, doi: 10.52710/cfs.867.

[10] T. A. Khan *et al.*, "Multi-Source Cyber Intrusion Detection Using Ensemble Machine Learning," *J. Comput. Sci.*, vol. 21, no. 1, pp. 111–123, Jan. 2025, doi: 10.3844/jcssp.2025.111.123.

[11] S. Singamsetty, "CyNet: Amalgam Deep Learning Model for Multi-Vector Cyber Intrusion Detection System (IDS)," in *2025 3rd International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI)*, IEEE, Sep. 2025, pp. 914–918. doi: 10.1109/ICoICI65217.2025.11253990.

[12] G. Modalavalasa, "Analysis and Optimization of Privacy-Preserving Encryption Techniques in Cloud Computing Environments for Secure Cloud Data," in *2025 5th International Conference on Intelligent Technologies (CONIT)*, IEEE, Jun. 2025, pp. 1–6. doi: 10.1109/CONIT65521.2025.11167685.

[13] A. Gupta, "What Is The Right Security Posture? A Perspective on Cloud Computing Security Threats and Risk Assessment," *Int. J. Emerg. Res. Eng. Technol.*, vol. 4, no. 4, pp. 120–127, December, 2023, doi: 10.63282/3050-922X.IJERET-V4I4P112.

[14] V. Shah, "Managing Security and Privacy in Cloud Frameworks : A Risk with Compliance Perspective for Enterprises," *Int. J. Curr. Eng. Technol.*, vol. 12, no. 6, pp. 606–618, 2022, doi: 10.14741/ijcet/v.12.6.16.

[15] A. R. Bilipelli, "AI-Driven Intrusion Detection Systems for Large-Scale Cybersecurity Networks Data Analysis : A Comparative Study," *TIJER – Int. Res. J.*, vol. 11, no. 12, pp. 922–928, 2024.

[16] A. Katangoori, "The Role of Big Data in Advancing Artificial Intelligence: Methods and Case Studies," *Int. J. Artif. Intell. Mach. Learn.*, vol. 6, no. 1, pp. 37–54, Jan. 2026, doi: 10.51483/IJAIML.6.1.2026.37-54.

[17] A. R. Toorpu, S. K. Vududala, A. Nerella, and B. P. Madupati, "Hybrid AI Models for Privacy-Preserving Big Data Analytics in Distributed Environments," in *2025 Global Conference in Emerging Technology (GINOTECH)*, IEEE, May 2025, pp. 1–8. doi: 10.1109/GINOTECH63460.2025.11076666.

[18] S. K. Chintagunta and S. Amrale, "Enhancing Cloud Database Security Through Intelligent Threat Detection and Risk Mitigation," *Tech. Int. J. Eng. Res.*, vol. 9, no. 10, pp. 49–55, May, 2022, doi: 10.56975/tijer.v9i10.159996.

[19] D. Bhattacharjee, "Design and Evaluation of Deep Generative AI Model for Intrusion Detection in Cyber Threat Monitoring," in *2025 7th International Symposium on Advanced Electrical and Communication Technologies (ISAECT)*, IEEE, Dec. 2025, pp. 1–6. doi: 10.1109/ISAECT68904.2025.11318752.

[20] G. Sarraf and V. Pal, "Autonomous Threat Detection and Response in Cloud Security: A Comprehensive Survey of AI-Driven Strategies," *Int. J. Emerg. Res. Eng. Technol.*, vol. 6, no. 4, 2025, doi: 10.63282/3050-922X.IJERET-V6I4P114.

[21] S. Thangavel, S. Srinivasan, S. B. V. Naga, and K. Narukulla, "Distributed Machine Learning for Big Data Analytics: Challenges, Architectures, and Optimizations," *Int. J. Artif. Intell. Data Sci. Mach. Learn.*, vol. 4, no. 3, pp. 18–30, 2023, doi: 10.63282/3050-9262.IJAIDSML-V4I3P103.

[22] P. Chandrashekar and M. Kari, "Design Machine Learning-Based Zero-Trust Intrusion Identification Models for Securing Cloud Computing System," *Int. J. Res. Anal. Rev.*, vol. 11, no. 4, pp. 901–907, 2024.

[23] S. Narang and A. Gogineni, "Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment," *Int. J. Sci. Res. Mod. Technol.*, vol. 4, no. 5, pp. 60–70, Jun. 2025, doi: 10.38124/ijsrmt.v4i5.542.

[24] A. K. Shukla, A. Sharma, and S. S. Sengar, "SACFFNet: Shuffle Attention Convolutional Forward Fractional Network Based Attack Detection in Cloud Computing," *Concurr. Comput. Pract. Exp.*, vol. 38, no. 3, pp. 1–18, Feb. 2026, doi: 10.1002/cpe.70504.

[25] X. Jiang, R. Jia, and F. Zhang, "Deep Learning-Based User Behavior Anomaly Detection and Threat Early Warning in Cloud Computing Environments," *Acad. Nexus J.*, vol. 4, no. 3, pp. 1–24, 2025.

[26] V. Mamidala, A. R. G. Yallamelli, M. V. Devarajan, T. Ganesan, R. K. M. K. Yalla, and A. Sambas, "Hybrid anomaly-based cloud security and machine learning-based behavioral analysis for threat intelligence detection in cloud environment," *Cluster Comput.*, vol. 28, no. 8, p. 485, Sep. 2025, doi: 10.1007/s10586-024-05025-x.

[27] T. A. Devi and A. Jain, "Enhancing Cloud Security with Deep Learning-Based Intrusion Detection in Cloud Computing Environments," in *2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT)*, IEEE, May 2024, pp. 541–546. doi: 10.1109/InCACCT61598.2024.10551040.

[28] D. Chaudhary, S. K. Verma, V. M. Shrimal, R. Madala, R. Baliyan, and S. M, "AI-Based Methods to Detect and Counter Cyber Threats in Cloud Environments to Strengthen Cloud Security," in *2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT)*, IEEE, Aug. 2024, pp. 1–6. doi: 10.1109/ICEECT61758.2024.10739173.

[29] P. Parameswarappa, T. Shah, and G. R. Lanke, "A Machine Learning-Based Approach for Anomaly Detection for Secure Cloud Computing Environments," in *2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, IEEE, Jan. 2023, pp. 931–940. doi: 10.1109/IDCIoT56793.2023.10053518.

[30] M. H. Zaib, "NSL-KDD," Kaggle. [Online]. Available: https://www.kaggle.com/datasets/hassan06/nslkdd

[31] Y. Muni, "A Review of Efficient Routing Architectures Using OSPF, BGP, and MPLS in Multi-Protocol Networks," *Eng. Technol. J.*, vol. 11, no. 01, Jan. 2026, doi: 10.47191/etj/v11i01.21.

[32] P. Nutalapati, J. R. Vummadi, S. Dodda, and N. Kamuni, "Advancing Network Intrusion Detection: A Comparative Study

of Clustering and Classification on NSL-KDD Data," in *2025 International Conference on Data Science and Its Applications (ICoDSA)*, Jakarta, Indonesia: IEEE, Jul. 2025, pp. 880–885. doi: 10.1109/ICoDSA67155.2025.11157595.

[33] S. B. Shah, B. Boddu, N. Prajapati, and S. A. Pahune, "AI-Powered Advanced Intrusion Detection for Securing Cloud Environments Against Network Attacks," in *2025 Global Conference in Emerging Technology (GINOTECH)*, IEEE, May 2025, pp. 1–7. doi: 10.1109/GINOTECH63460.2025.11076673.

[34] S. Garg, "Predictive Analytics and Auto Remediation using Artificial Inteligence and Machine learning in Cloud Computing Operations," 2025, *SSRN*. doi: 10.2139/ssrn.5267117.

[35] M. R. R. Deva and N. Jain, "Utilizing Azure Automated Machine Learning and XGBoost for Predicting Cloud Resource Utilization in Enterprise Environments," in *2025 International Conference on Networks and Cryptology (NETCRYPT)*, IEEE, May 2025, pp. 535–540. doi: 10.1109/NETCRYPT65877.2025.11102235.

[36] D. Patel, "Zero Trust and DevSecOps in Cloud-Native Environments with Security Frameworks and Best Practices," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, pp. 454–464, Jan. 2024, doi: 10.48175/IJARSCT-11900D.

[37] H. Attou *et al.*, "Towards an Intelligent Intrusion Detection System to Detect Malicious Activities in Cloud Computing," *Appl. Sci.*, vol. 13, no. 17, p. 9588, Aug. 2023, doi: 10.3390/app13179588.

[38] A. Isong, B. U. Stephen, P. Asuquo, C. Ihemereze, and I. Enang, "Machine Learning Based Cloud Computing Intrusion Detection," *Adv. Inf. Syst.*, vol. 10, no. 1, pp. 115–125, Jan. 2026, doi: 10.20998/2522-9052.2026.1.13.

[39] A. Alshammari and A. Aldribi, "Apply machine learning techniques to detect malicious network traffic in cloud computing," *J. Big Data*, vol. 8, no. 1, p. 90, Dec. 2021, doi: 10.1186/s40537-021-00475-1.

[40] P. O. Prakash, K. Sasirekha, and D. Vistro, "A DDOS prevention system designed using machine learning for cloud computing environ-ment," *Int. J. Manag.*, vol. 11, no. 10, pp. 1797–1806, 2020, doi: 10.34218/IJM.11.10.2020.167.