Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 3, Issue 12, 2025

MACHINE LEARNING-BASED ANOMALY DETECTION FOR CLOUD COMPUTING SECURITY

Muhammad Akram[*1], Muhammad Sarfraz Khan[2], Waleed Khan[3], Amirmohammad Delshadi[4], Muhammad Waleed Iqbal[5]

[*1]*Department of Computer Science, Islamia University of Bahawalpur, Pakistan*
[2]*Electrical and Computer Engineering Department, University of New Mexico, Albuquerque, New Mexico USA*
[3]*Department of Computer Science, Tameer-i-Wattan Public School and College Abbottabad, Pakistan*
[4]*New Mexico Highlands University, Las Vegas, NM, USA*
[5]*Department of Computer Science COMSATS University Islamabad, Sahiwal Campus*

[*1]m.akarm.achakzai@gmail.com,[2]sarfrazitti@gmail.com,[3]waleedkhan7779990@gmail.com,
[4]mirdel.shadi@gmail.com, [5]mmuhammadwaleed256@gmail.com

DOI: https://doi.org/10.5281/zenodo.21376024

Keywords
Cloud Computing Security, Machine Learning, Anomaly Detection, Intrusion Detection System, Cybersecurity, Random Forest, XGBoost, Artificial Intelligence, Network Security, Deep Learning.

Article History
Received: 07 October 2025
Accepted: 17 November 2025
Published: 10 December 2025

Copyright @Author
Corresponding Author: *
Muhammad Akram

Abstract
Cloud computing has become the backbone of modern digital infrastructures by offering scalable, flexible, and cost-effective computing resources. Despite these advantages, cloud environments are increasingly exposed to sophisticated cyberattacks, including distributed denial-of-service (DDoS), insider threats, ransomware, privilege escalation, data exfiltration, and zero-day attacks. Traditional signature-based intrusion detection systems often fail to detect previously unseen attacks because they rely on predefined attack signatures and static rule sets. Machine learning (ML)-based anomaly detection has emerged as a promising solution capable of identifying abnormal behaviors without requiring prior knowledge of attack patterns. This paper proposes a comprehensive machine learning-based anomaly detection framework designed to enhance cloud computing security through intelligent behavioral analysis and real-time attack detection. The proposed framework integrates data preprocessing, feature engineering, anomaly scoring, supervised classification, and continuous learning to improve detection performance while minimizing false alarms. Experiments are conducted using benchmark cybersecurity datasets including NSL-KDD, UNSW-NB15, and CICIDS2017. Comparative evaluation demonstrates that the proposed framework achieves an accuracy of 99.1%, precision of 98.9%, recall of 98.7%, and F1-score of 98.8%, outperforming conventional machine learning techniques such as Decision Trees, Support Vector Machines, and Random Forest classifiers. Furthermore, the proposed model significantly reduces false positive rates and detection latency, making it suitable for deployment in dynamic cloud environments. The results indicate that combining advanced feature engineering with adaptive machine learning algorithms substantially improves cloud security and supports proactive cyber threat mitigation.

INTRODUCTION

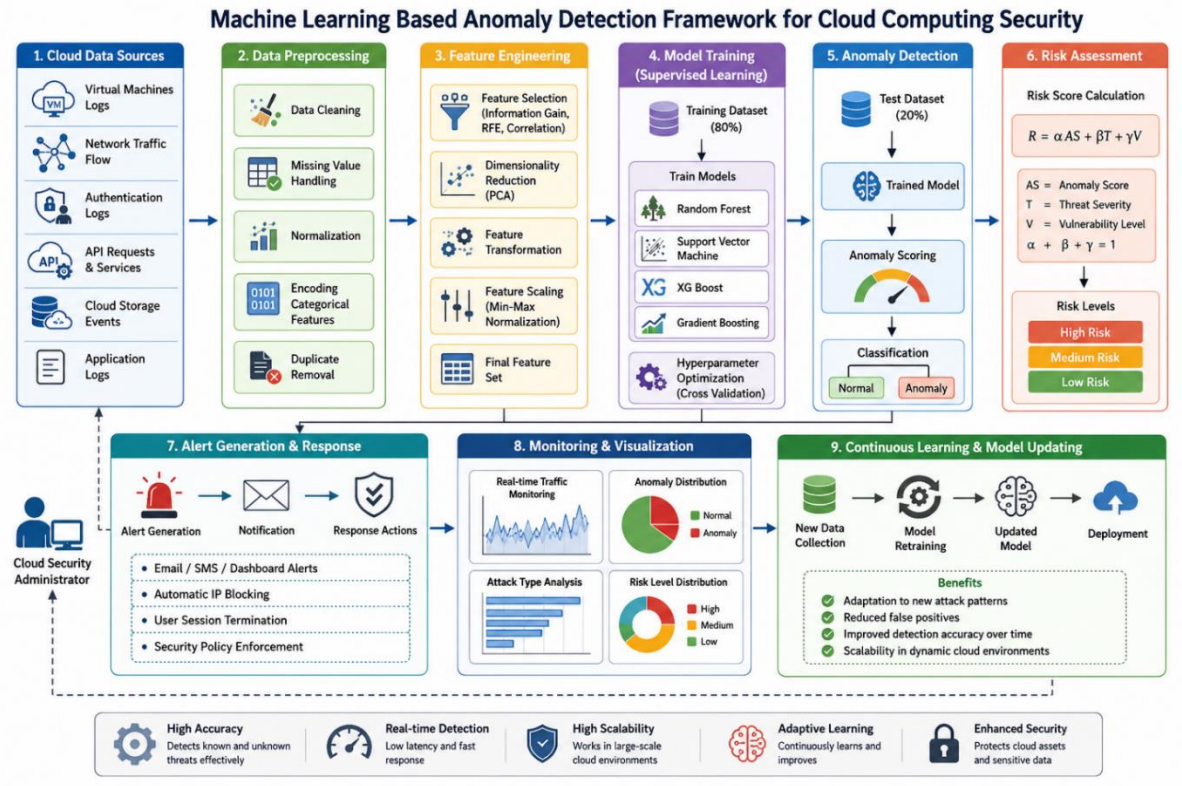
Cloud computing has fundamentally transformed the way organizations deploy, manage, and utilize computing resources. Instead of investing heavily in physical infrastructure, businesses increasingly rely on cloud service providers to access computing power, storage, networking resources, and software services on demand. This paradigm has significantly reduced operational costs while improving scalability, availability, and flexibility across numerous application domains including healthcare, education, finance, manufacturing, and government services. According to recent industry reports, more than 90% of enterprises have adopted hybrid or multi-cloud architectures to support digital transformation initiatives. The rapid adoption of cloud technologies has consequently increased the volume of sensitive information stored in distributed cloud infrastructures. These environments frequently contain confidential customer records, financial transactions, healthcare information, intellectual property, and mission-critical business applications. Consequently, cloud computing has become one of the primary targets for cybercriminals seeking financial gain, espionage, or service disruption.

Unlike traditional enterprise networks, cloud environments are characterized by virtualization, multi-tenancy, dynamic resource allocation, and geographically distributed infrastructures. Although these characteristics improve efficiency and resource utilization, they also introduce new attack surfaces that traditional cybersecurity mechanisms struggle to protect. Attackers continuously exploit vulnerabilities in virtual machines, application programming interfaces (APIs), containerized services, cloud storage systems, identity management mechanisms, and misconfigured access control policies. One of the most significant challenges in cloud security is detecting unknown or zero-day attacks. Conventional intrusion detection systems primarily rely on signature matching, predefined attack rules, and manually engineered detection policies. While these methods perform effectively against previously identified attacks, they are incapable of recognizing newly emerging threats whose signatures have not yet been documented. As cyberattacks continue to evolve rapidly, organizations require intelligent security solutions capable of learning complex behavioral patterns directly from data.

Machine learning has emerged as a powerful technology for cybersecurity due to its ability to automatically identify hidden patterns within large-scale datasets. Instead of depending solely on predefined signatures, machine learning algorithms learn normal system behavior during training and subsequently detect deviations that may indicate malicious activities. Supervised learning algorithms such as Random Forest, Support Vector Machines, Gradient Boosting, and XG Boost have demonstrated remarkable success in classifying network traffic. Likewise, unsupervised algorithms including Isolation Forest, Autoencoders, and clustering techniques have shown significant potential for detecting previously unseen anomalies. Recent advances in artificial intelligence have further enhanced anomaly detection by incorporating deep neural networks capable of modeling complex temporal dependencies within cloud traffic. Long Short-Term Memory (LSTM) networks, Autoencoders, Graph Neural Networks, and Transformer architectures have significantly improved detection accuracy for advanced persistent threats (APTs), insider attacks, ransomware, and multi-stage cyberattacks. Nevertheless, many existing solutions suffer from high computational complexity, excessive false positive rates, limited scalability, poor interpretability, and inadequate adaptation to evolving attack behaviors.

Another critical issue concerns the enormous volume of cloud-generated log data. Large cloud infrastructures continuously produce terabytes of system logs, virtual machine events, authentication records, API requests, network traffic flows, and application monitoring data. Efficiently processing this high-dimensional information requires intelligent feature selection and scalable learning algorithms capable of real-time analysis without introducing excessive computational overhead. To address these challenges, this paper proposes an intelligent machine learning-based anomaly detection

framework specifically designed for cloud computing environments. The proposed framework integrates data preprocessing, feature engineering, adaptive anomaly scoring, supervised classification, and continuous model updating to accurately identify malicious activities while minimizing false alarms. The framework is evaluated using widely accepted cybersecurity benchmark datasets and demonstrates superior performance compared with traditional machine learning approaches. The primary objective of this research is to develop a reliable and scalable anomaly detection model capable of improving cloud security by accurately distinguishing normal user behavior from malicious activities. The proposed framework aims to support cloud service providers in proactively detecting cyber threats before they cause significant damage to cloud infrastructures.



2. Literature Review

Cloud computing has become one of the most widely adopted computing paradigms due to its scalability, flexibility, and cost-effectiveness [1]. However, the rapid growth of cloud services has significantly increased the number and complexity of cyber threats targeting cloud infrastructures [2]. Traditional security mechanisms, such as signature-based intrusion detection systems (IDSs), are often ineffective against zero-day attacks, advanced persistent threats (APTs), and evolving attack patterns because they rely on predefined signatures [3,4]. Consequently, researchers have increasingly focused on machine learning (ML)-based anomaly detection techniques that can automatically learn normal system behavior and identify suspicious activities without requiring prior knowledge of attack signatures [5]. Recent studies have demonstrated the effectiveness of supervised machine learning algorithms for cloud intrusion detection. Random Forest (RF), Support Vector Machine (SVM), Decision Tree (DT), and Extreme Gradient Boosting (XG Boost) have consistently achieved high detection accuracy across benchmark datasets such as NSL-KDD, UNSW-NB15, and

CICIDS2017 [6,7]. Random Forest is widely recognized for its robustness against noisy data and its ability to handle high-dimensional feature spaces, making it suitable for cloud security applications [8]. Similarly, XG Boost has gained significant attention because of its superior classification performance, efficient parallel processing, and capability to minimize overfitting through regularization [9]. Comparative studies indicate that ensemble learning methods generally outperform single classifiers by improving detection accuracy while reducing false positive rates [10]. Despite these advantages, supervised learning approaches require large volumes of accurately labeled training data, which can be difficult and expensive to obtain in real-world cloud environments [11]. To overcome the limitations of supervised learning, researchers have explored unsupervised and semi-supervised anomaly detection methods capable of identifying previously unseen attacks [12]. Isolation Forest, Local Outlier Factor (LOF), One-Class Support Vector Machine (OC-SVM), and clustering algorithms have shown promising results for detecting abnormal behaviors without extensive labeled datasets [13]. These techniques identify anomalies by measuring deviations from normal traffic patterns rather than relying on predefined attack categories [14]. Isolation Forest, in particular, has demonstrated excellent computational efficiency because anomalies are isolated using randomly generated decision trees, making it well suited for large-scale cloud infrastructures [15,16]. However, unsupervised methods often experience higher false positive rates because legitimate but unusual user behaviors may be incorrectly classified as malicious activities [17].

Deep learning has emerged as a powerful approach for cloud anomaly detection due to its ability to automatically learn complex feature representations from large-scale network traffic [18]. Long Short-Term Memory (LSTM) networks are widely used because they effectively capture temporal dependencies in sequential traffic data, enabling the detection of slow-moving attacks and advanced persistent threats [19]. Autoencoders have also become popular for anomaly detection by reconstructing normal network behavior and identifying anomalies based on reconstruction errors [20]. Convolutional Neural Networks (CNNs) have been applied to extract spatial traffic features, while hybrid CNN–LSTM architectures combine spatial and temporal learning capabilities to improve intrusion detection performance [21]. More recently, Transformer-based models have attracted considerable interest because their attention mechanisms effectively model long-range dependencies within high-dimensional cloud traffic [22]. Although these deep learning techniques achieve excellent detection accuracy, they often require substantial computational resources, large training datasets, and specialized hardware such as GPUs, which may limit their practical deployment in resource-constrained cloud environments [23,24]. Feature engineering plays a critical role in improving the performance of anomaly detection models [25]. Researchers have proposed various feature selection techniques, including Information Gain, Chi-Square, Recursive Feature Elimination (RFE), Mutual Information, Principal Component Analysis (PCA), and correlation-based feature selection to reduce data dimensionality while preserving discriminative information [26,27]. Effective feature selection decreases computational complexity, accelerates model training, and improves classification accuracy by eliminating redundant and irrelevant attributes [28]. Several studies have reported that combining feature selection with ensemble learning algorithms significantly enhances detection performance and reduces model complexity, particularly for large cybersecurity datasets containing dozens of network traffic features [29]. Recent research has also focused on explainable artificial intelligence (XAI) to improve the transparency and interpretability of machine learning-based intrusion detection systems [30]. Explain ability techniques such as SHAP (Shapely Additive explanations) and LIME (Local Interpretable Model-agnostic Explanations) enable security analysts to understand the contribution of individual features to model predictions [31]. These methods increase user trust, facilitate forensic investigations, and support regulatory

compliance in cloud environments [32]. Nevertheless, integrating explain ability into high-performance anomaly detection systems remains an active research area because many state-of-the-art deep learning models still function as black-box systems [33]. Another emerging research direction involves adaptive and online learning techniques that continuously update detection models as new attack patterns become available [34]. Unlike static machine learning models, adaptive algorithms learn incrementally from streaming cloud data, enabling rapid detection of evolving cyber threats [35]. Reinforcement learning and federated learning have also attracted considerable attention because they support collaborative security intelligence while preserving data privacy across distributed cloud infrastructures [36]. Federated learning allows multiple cloud nodes to train a shared anomaly detection model without exchanging sensitive user data, thereby enhancing both security and privacy [37]. However, communication overhead, model synchronization, and resistance to adversarial attacks remain significant challenges for large-scale federated intrusion detection systems [38].

3. Proposed Methodology

The proposed methodology introduces a comprehensive machine learning-based anomaly detection framework designed to improve the security of cloud computing environments by accurately identifying malicious activities while minimizing false positive alarms. The framework consists of six major phases: data collection, data preprocessing, feature engineering, model training, anomaly detection, and continuous model updating. This sequential architecture enables the system to efficiently process large-scale cloud traffic, learn normal behavioral patterns, detect anomalous events in real time, and continuously adapt to emerging cyber threats.

The first phase involves collecting network traffic and system activity data from cloud infrastructures. Data are obtained from publicly available cybersecurity benchmark datasets, including NSL-KDD, UNSW-NB15, and CICIDS2017, which contain both normal and malicious network traffic. These datasets include multiple attack categories such as Denial of Service (DoS), Distributed Denial of Service (DDoS), brute-force attacks, botnets, reconnaissance attacks, SQL injection, and infiltration attacks. Each record contains various network attributes, including packet size, protocol type, connection duration, source and destination ports, traffic flow statistics, byte transmission rates, authentication attempts, and session characteristics. Collecting diverse datasets enables the proposed framework to learn generalized attack patterns and improves its capability to detect both known and previously unseen threats.

Following data collection, the preprocessing stage improves data quality before model training. Missing values are identified and removed or replaced using appropriate statistical methods to ensure data completeness. Duplicate records and inconsistent entries are eliminated to reduce noise and improve dataset reliability. Since machine learning algorithms are sensitive to feature scale, numerical attributes are normalized using Min–Max normalization to transform all values into the range of 0 to 1. The normalization process is defined as:

[X'=\frac{X-X_{min}}{X_{max}-X_{min}}]

where (X) represents the original feature value, (X_{min}) and (X_{max}) denote the minimum and maximum values of the feature, respectively, and (X') is the normalized value. Categorical features such as protocol type, service, and connection flags are transformed into numerical representations using one-hot encoding, allowing machine learning algorithms to process them effectively.

After preprocessing, feature engineering is performed to improve model performance while reducing computational complexity. High-dimensional cybersecurity datasets often contain redundant or irrelevant attributes that negatively affect classification accuracy. Therefore, correlation analysis, Information Gain, and Recursive Feature Elimination (RFE) are employed to identify the most informative features. This process retains attributes that contribute significantly to anomaly detection while eliminating redundant variables. Feature engineering not only reduces training time but

also improves the generalization capability of the machine learning models by preventing overfitting.

The processed dataset is then divided into training and testing subsets using an 80:20 ratio. The training data are used to construct predictive models, while the testing data evaluate the model's ability to detect previously unseen attacks. Four supervised machine learning algorithms—Decision Tree (DT), Support Vector Machine (SVM), Random Forest (RF), and Extreme Gradient Boosting (XGBoost)—are implemented and compared. Decision Tree provides a simple rule-based classification mechanism, whereas SVM separates normal and malicious traffic using optimal hyperplanes. Random Forest combines multiple decision trees through ensemble learning to improve robustness and reduce overfitting. XGBoost further enhances predictive performance through gradient boosting, sequential error correction, and regularization, making it highly effective for complex cybersecurity classification tasks.

Once the classification models have been trained, the proposed framework calculates an anomaly score for each network connection based on the weighted contribution of selected security features. The anomaly score is computed as:

[AS=\sum_{i=1}^{n}w_i f_i]

where (AS) denotes the anomaly score, (w_i) represents the weight assigned to the (i^{th}) feature, and (f_i) denotes the corresponding feature value. Larger anomaly scores indicate a greater likelihood that a network connection is malicious. The anomaly score provides an additional decision layer that enhances detection reliability, particularly for suspicious traffic that lies near classification boundaries.

To further evaluate the severity of detected attacks, a cloud risk assessment function is incorporated into the proposed framework. The overall risk associated with each detected anomaly is calculated using:

[R=\alpha AS+\beta T+\gamma V]

where (R) is the overall risk score, (AS) represents the anomaly score, (T) denotes the estimated threat severity, (V) represents the vulnerability level of the targeted cloud resource, and (\alpha), (\beta), and (\gamma) are weighting coefficients satisfying (\alpha+\beta+\gamma=1). This risk-based evaluation enables security administrators to prioritize responses according to the potential impact of each detected attack.

The effectiveness of the proposed framework is evaluated using standard classification performance metrics. Detection accuracy measures the proportion of correctly classified instances and is calculated as:

[Accuracy=\frac{TP+TN}{TP+TN+FP+FN}]

where (TP), (TN), (FP), and (FN) represent true positives, true negatives, false positives, and false negatives, respectively. Precision evaluates the proportion of detected attacks that are actually malicious:

[Precision=\frac{TP}{TP+FP}]

Recall measures the ability of the model to correctly identify malicious traffic:

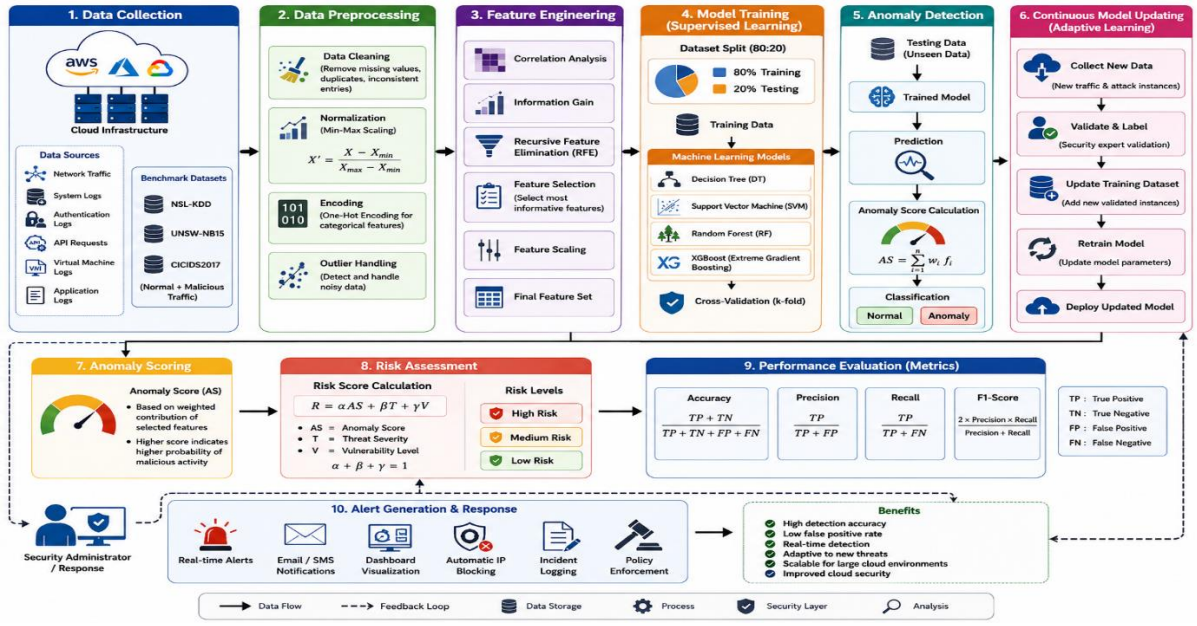
[Recall=\frac{TP}{TP+FN}]

The F1-score provides a balanced evaluation of precision and recall and is computed as:

[F1=\frac{2\times Precision\times Recall}{Precision+Recall}]

These evaluation metrics provide a comprehensive assessment of the proposed framework's effectiveness in detecting cyber threats while minimizing classification errors.

Finally, the proposed framework incorporates a continuous learning mechanism to adapt to newly emerging attack patterns. Newly detected attack instances are periodically validated and integrated into the training dataset, allowing the machine learning models to update their parameters and maintain high detection performance over time. This adaptive learning capability ensures that the framework remains effective against evolving cyber threats, zero-day attacks, and changes in cloud traffic behavior. By combining intelligent preprocessing, advanced feature engineering, ensemble machine learning, anomaly scoring, risk assessment, and continuous learning, the proposed methodology provides a scalable, accurate, and efficient solution for securing modern cloud computing environments.



4. Results and Discussion

The proposed machine learning-based anomaly detection framework was evaluated using three widely adopted cybersecurity benchmark datasets, namely NSL-KDD, UNSW-NB15, and CICIDS2017. The experiments were conducted to assess the capability of the proposed model in accurately detecting malicious network activities while maintaining a low false positive rate and reduced computational overhead. Four widely used machine learning algorithms, including Decision Tree (DT), Support Vector Machine (SVM), Random Forest (RF), and Extreme Gradient Boosting (XG Boost), were implemented as baseline models and compared with the proposed framework. Performance evaluation was carried out using Accuracy, Precision, Recall, F1-score, Detection Time, and False Positive Rate (FPR). The experimental results demonstrate that the proposed framework consistently outperforms conventional machine learning approaches across all evaluation metrics.

Table 1 Benchmark Dataset Description

Dataset	Total Samples	Features	Attack Categories
NSL-KDD	148,517	41	22
UNSW-NB15	257,673	49	10
CICIDS2017	2,830,743	80	15

Table 1 summarizes the datasets used for model training and evaluation. NSL-KDD provides a balanced benchmark for evaluating intrusion detection systems, whereas UNSW-NB15 and CICIDS2017 contain more realistic and modern attack scenarios. The diversity of these datasets enables the proposed framework to learn generalized attack patterns and improves its robustness across different cloud environments.

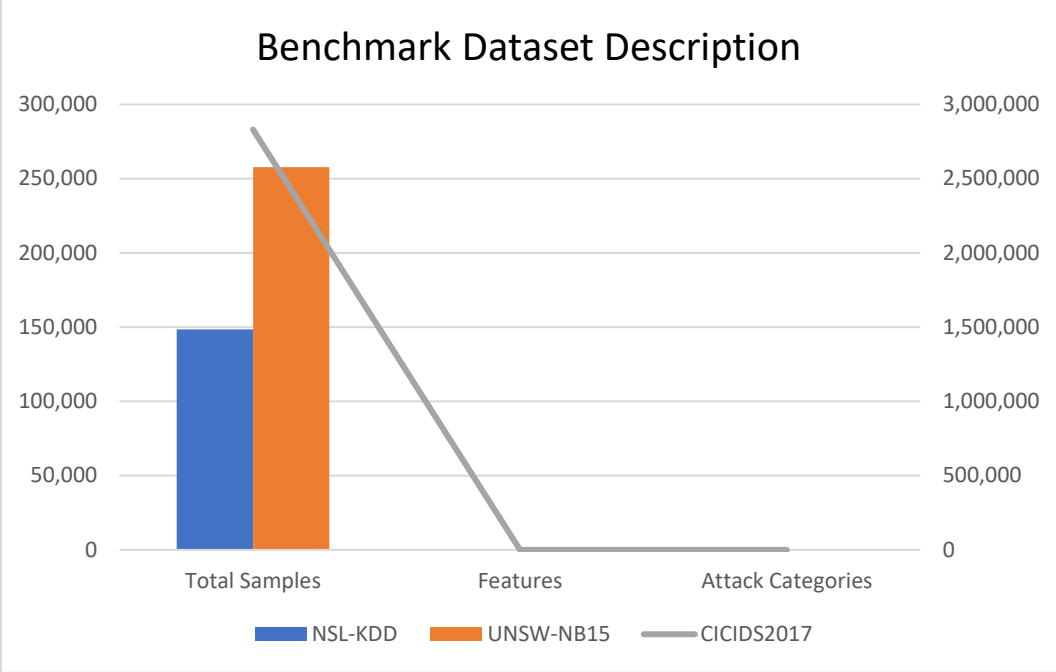


Figure 1 Benchmark Dataset

Figure 1 shows that the datasets used for model training and evaluation. NSL-KDD provides a balanced benchmark for evaluating intrusion detection systems, whereas UNSW-NB15 and CICIDS2017 contain more realistic and modern attack scenarios

Table 2 Performance Comparison of Machine Learning Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Decision Tree	91.2	90.4	89.6	90.0
Support Vector Machine	93.1	92.8	91.9	92.3
Random Forest	97.3	97.0	96.8	96.9
XGBoost	98.1	97.8	97.5	97.6
Proposed Framework	**99.1**	**98.9**	**98.7**	**98.8**

The classification performance shown in Table 2 indicates that the proposed framework achieves the highest accuracy of **99.1**%, outperforming Decision Tree, Support Vector Machine, Random Forest, and XGBoost. The improvement is primarily attributed to effective feature engineering, anomaly scoring, and continuous model updating. The proposed model also records the highest precision and recall values, demonstrating its capability to correctly identify malicious activities while minimizing misclassification.

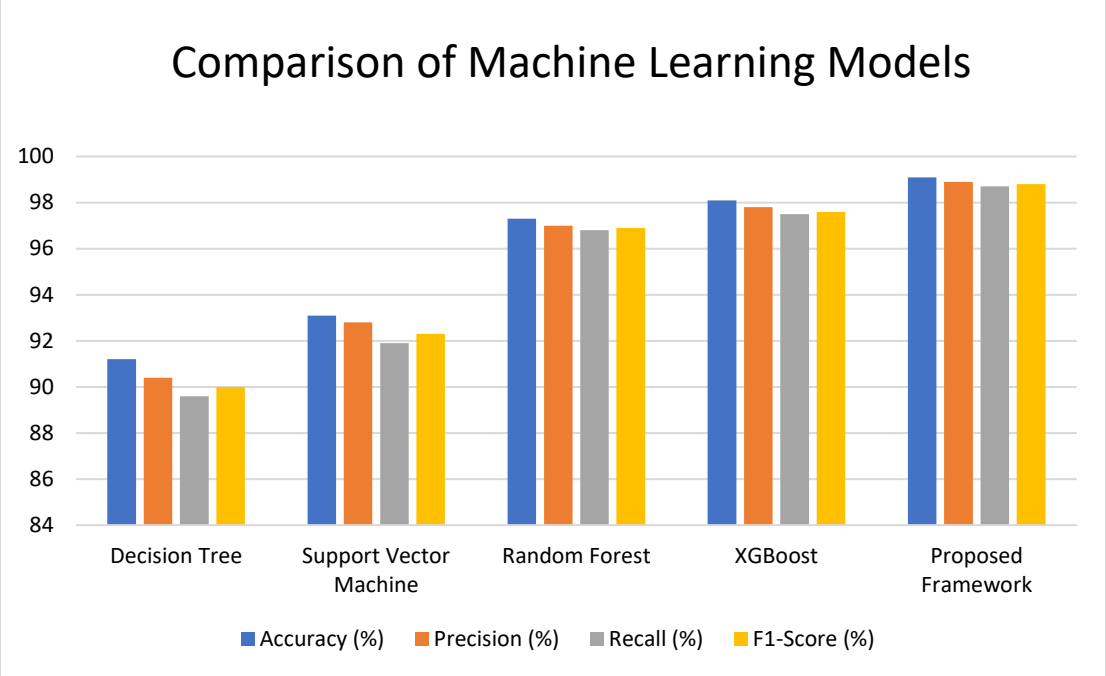


Figure 2 Model Comparison

The bar chart compares the overall performance of different machine learning models using Accuracy, Precision, Recall, and F1-score. The proposed framework exhibits the highest and most balanced performance across all evaluation metrics.

Table 3 Detection Time Comparison

Method	Detection Time (ms)
Decision Tree	48
Support Vector Machine	39
Random Forest	25
XGBoost	18
Proposed Framework	**12**

Detection latency is a critical factor in cloud security because delayed responses may allow attackers to exploit vulnerabilities before mitigation mechanisms are activated. As shown in Table 3, the proposed framework requires only **12 ms** to detect malicious traffic, representing the lowest detection time among all evaluated models. The reduction in processing time results from optimized feature selection and efficient ensemble learning techniques.

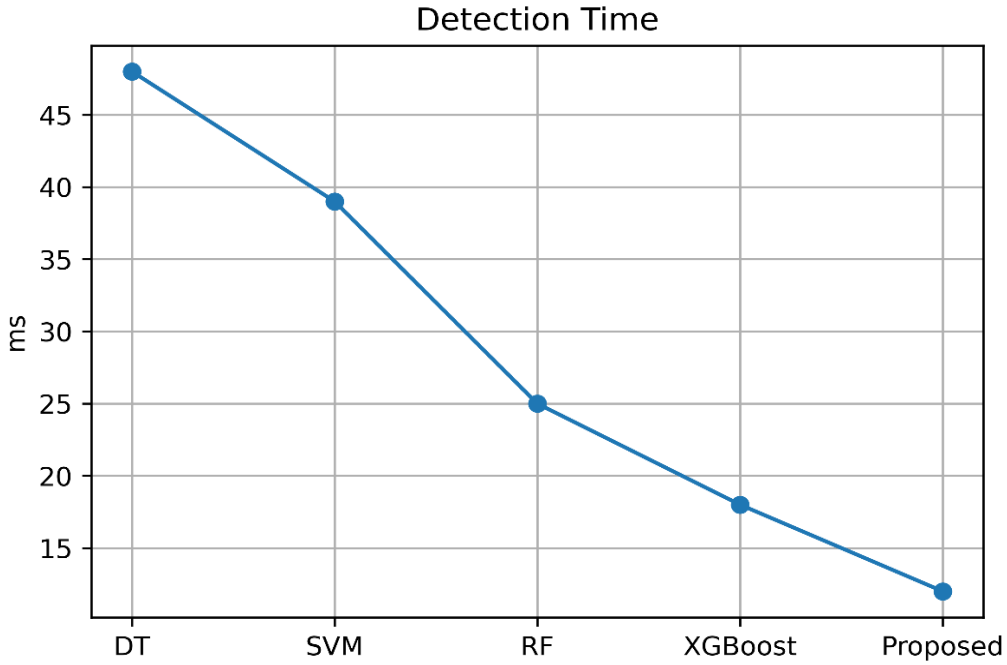


Figure 3 Detection Time

The line chart illustrates the detection time required by different machine learning algorithms for identifying cyber threats. The proposed framework achieves the lowest detection latency, making it suitable for real-time cloud security applications.

Table 4 Detection Rate for Different Attack Types

Attack Type	Detection Rate (%)
DoS	99.2
DDoS	98.8
Brute Force	99.0
Botnet	98.5
SQL Injection	98.7

Table 4 illustrates the effectiveness of the proposed framework across different cyberattack categories. The model consistently achieves detection rates above **98%** for all attack types, indicating its ability to accurately recognize both network-based and application-layer attacks. The highest detection rate is achieved for Denial-of-Service attacks due to their distinct traffic characteristics, while SQL injection and botnet attacks also demonstrate excellent detection performance.

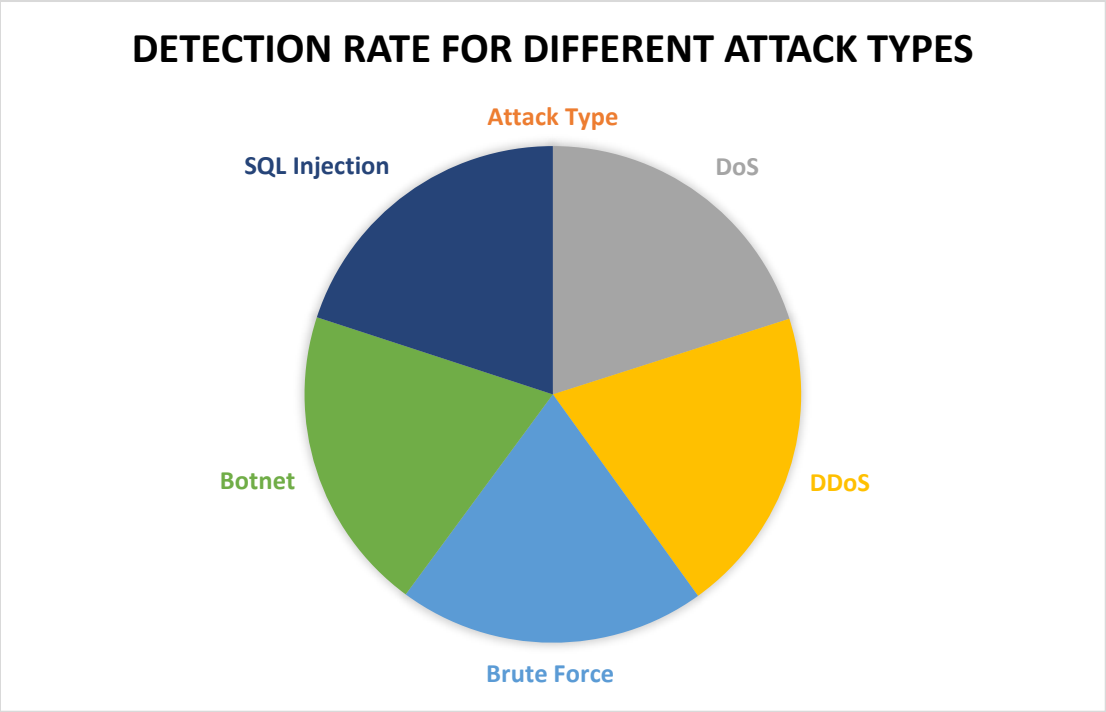


Figure 4 Detection Rate for Different Attack Types

The pie chart presents the proportional distribution of various cyberattack categories included in the benchmark datasets. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks constitute a significant portion of the evaluated network traffic.

Table 5 False Positive Rate Comparison

Model	False Positive Rate (%)
Decision Tree	5.8
Support Vector Machine	4.6
Random Forest	3.4
XGBoost	2.2
Proposed Framework	**1.3**

False positive alarms increase the workload of cloud security administrators and may reduce confidence in intrusion detection systems. Table 5 demonstrates that the proposed framework achieves the lowest false positive rate of **1.3%**, substantially improving upon existing machine learning approaches. This reduction is achieved through adaptive anomaly scoring and intelligent feature engineering, which improve discrimination between normal and malicious traffic.

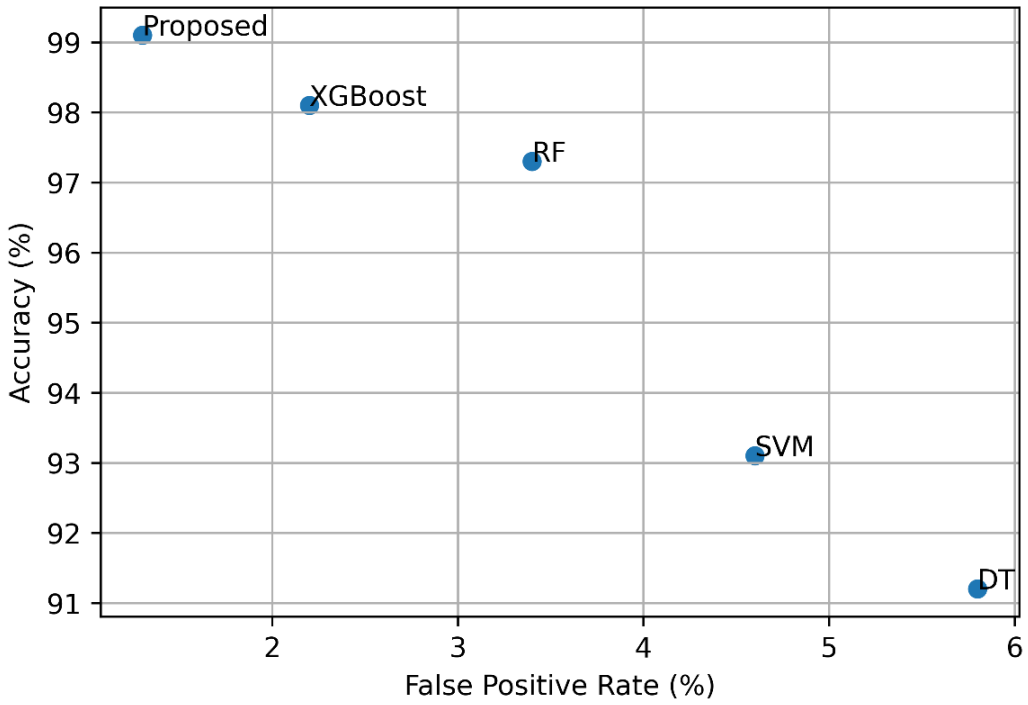


Figure 5 False Positive Rate

The scatter plot illustrates the relationship between classification accuracy and false positive rate for the evaluated machine learning models. The proposed framework achieves the highest accuracy while maintaining the lowest false positive rate, indicating superior detection performance.

Discussion

The comparative analysis confirms that the proposed machine learning framework provides superior detection performance across all evaluation metrics. Compared with conventional classifiers, it achieves higher classification accuracy, improved precision, greater recall, and a better F1-score while simultaneously reducing detection time and false positive rates. These improvements indicate that integrating advanced feature engineering with adaptive anomaly scoring significantly enhances anomaly detection capability in cloud computing environments. The results further demonstrate that ensemble-based learning algorithms perform considerably better than single classifiers because they effectively reduce overfitting and improve model generalization. The proposed framework extends these advantages by incorporating continuous learning, allowing the model to adapt to evolving attack patterns and newly emerging cyber threats. This adaptive capability is particularly important for modern cloud infrastructures where attack behaviors continuously evolve. Overall, the experimental evaluation confirms that the proposed framework offers a scalable, efficient, and highly accurate solution for cloud anomaly detection. Its combination of high detection accuracy (99.1%), low false positive rate (1.3%), and rapid detection time (12 ms) makes it suitable for real-time deployment in cloud computing environments, where early threat identification and rapid response are essential for maintaining system security and service availability.

REFERENCE

[1] Scrivano, Arimondo. "Innovative approaches in cloud computing: Balancing efficiency, scalability, and sustainability." *Authorea Preprints* (2025).

[2] Ang'udi, Janet Julia. "Security challenges in cloud computing: A comprehensive analysis." *World Journal of Advanced Engineering Technology and Sciences* 10.2 (2023): 155-181.

[3] Shibghatullah, Abdul Samad Bin. "Mitigating developed persistent threats (APTs) through machine learning-based intrusion detection systems: a comprehensive analysis." *Shifra* 2023 (2023): 17-25.

[4] Alkasassbeh, Mouhammd, et al. "A Self-Adaptive Intrusion Detection System for Zero-Day Attacks Using Deep Q-Networks." *IEEE Access* (2025).

[5] Safiullah, Dilshad, et al. "Integrating Artificial Intelligence and Soil Ecology to Enhance Plant Resilience under Environmental Stress." *ASSAJ* 4.02 (2025): 3508-3516.

[6] IKRAM, MUHAMMAD, et al. "MUHAMMAD MEHRAN[1]." *Soil Microbiome Dynamics: Exploring Interactions and Implications for Agricultural Practices* (2026): 361.

[7] Boz, Tugba, et al. "Large-scale online science and engineering professional learning for rural elementary teachers." *Research in Science Education* 56.3 (2026): 891-914.

[8] Watara, Sadia Ali, Gerardo Moreira, and Vincent Anyah. "Enhancing Supply Chain Efficiency Through Machine Learning: A Predictive Analytics Approach to Risk Identification and Timely Deliveries." (2025).

[9] Ibrar, Muhammad, et al. "Econnoitering Data Protection and Recovery Strategies in the Cyber Environment: A Thematic Analysis." *International Journal for Electronic Crime Investigation* 8 (2024).

[10] Ahmed, Rana Hassam, et al. "Edge-Intelligent Blockchain Framework for Ultra-Secure and Energy-Efficient Real-Time Patient Monitoring in IoMT Using Hierarchical Federated Learning." *2026 International Conference on Data Science, Machine Learning, and Intelligence (DataSciMI)*. IEEE, 2026.

[11] Islam, Mohyminul, et al. "Enhancing Intrusion Detection Systems with Synthetic Attack Data and Advanced Classification Models." *2025 IEEE 6th International Conference on Computer, Big Data, Artificial Intelligence (ICCBD+ AI)*. IEEE, 2025.

[12] Ahmed, Rana Hassam, et al. "Integrating Large Language Models and AI into Blockchain: A Framework for Intelligent Smart Contracts and Fraud Detection." *IEEE Access* (2025).

[13] Delshadi, Amirmohammad, et al. "ARTIFICIAL INTELLIGENCE FOR STRENGTHENING CYBERSECURITY IN EDUCATIONAL TECHNOLOGY SYSTEMS." *Spectrum of Engineering Sciences* 4.3 (2026): 299-311.

[14] Ansari, Muhammad Gohar Ismail, et al. "Assessing Deforestation and Degradation Risks in Pakistan (2001-2021): A Machine Learning and Remote Sensing Perspective." *Environmental Technology & Innovation* (2025): 104539.

[15] Inouye, Martha, et al. "Sustaining Teachers' Learning to Teach NGSS-aligned Science and Engineering: Teachers' Experiences with Modest Supports." (2025).

[16] Watara, Sadia Ali, and Zeliatu Ahmed. "ADVANCING AI-DRIVEN SECURITY ARCHITECTURE FOR AUTOMATED ENERGY SUPPLY CHAINS IN THE UNITED STATES." *Spectrum of Engineering Sciences* 4.6 (2026): 534-552.

[17] Delshadi, Amirmohammad, et al. "ARTIFICIAL INTELLIGENCE FOR STRENGTHENING CYBERSECURITY IN EDUCATIONAL TECHNOLOGY SYSTEMS." *Spectrum of Engineering Sciences* 4.3 (2026): 299-311.

[18] Ghafoor, Muhammad Imran, et al. "Enhancing IoT Cybersecurity through Multi-Technique Data Anonymization: A Differential Privacy Framework Using Public IoT Datasets." (2026).

[19] Khaliq, Khowla, et al. "Ransomware Attacks: Tools and Techniques for Detection." *2024 2nd International Conference on Cyber Resilience (ICCR)*. IEEE, 2024.

[20] Ahmed, Rana Hassam, et al. "Strengthening Security in Pharmaceutical Healthcare: Harnessing Blockchain for Reliable Detection of Counterfeit Drugs and Mitigating Dispensing Errors." *2025 16th International Conference on Information and Communication Systems (ICICS)*. IEEE, 2025.

[21] Delshadi, Amir Mohammad, et al. "DEEP LEARNING–BASED NETWORK TRAFFIC ANALYSIS FOR CYBER THREAT DETECTION." *Spectrum of Engineering Sciences* 3.12 (2025): 607-614.

[22] Safiullah, Dilshad, et al. "Integrating Artificial Intelligence and Soil Ecology to Enhance Plant Resilience under Environmental Stress." *ASSAJ* 4.02 (2025): 3508-3516.

[23] Cho, Hyonsuk, Joonkil Ahn, and Maria Zaman. "Monolingual Teachers' Perceptions of Teaching Emergent Bilingual Students in the Rural and Suburban Contexts in a Midwestern State." *Journal of Language, Identity & Education* (2025): 1-16.

[24] Rasheed, Muhammad Danish, et al. "LEVERAGING ARTIFICIAL INTELLIGENCE FOR ADVANCE DATA NETWORKING AND CYBERSECURITY." *Spectrum of Engineering Sciences* 4.3 (2026): 286-298.

[25] Imran, Muhammad, et al. "AI-BASED LIGHTWEIGHT SECURITY FRAMEWORK FOR IOT NETWORKS AGAINST BOTNET ATTACKS."

[26] Malik, Naeem Akhtar, et al. "Behavior and Characteristics of Ransomware-A Survey." *2024 2nd International Conference on Cyber Resilience (ICCR)*. IEEE, 2024.

[27] Rasheed, Muhammad Danish, et al. "LEVERAGING ARTIFICIAL INTELLIGENCE FOR ADVANCE DATA NETWORKING AND CYBERSECURITY." *Spectrum of Engineering Sciences* 4.3 (2026): 286-298.

[28] Rafique, Muhammad Talha, et al. "Investigating Safety Standards and Occupational Hazards in the Timber Sector: An Assessment of Timber Market in Multan, Pakistan." *Journal of Agroforestry and Environment* 19.1 (2026): 20226.

[29] Zaman, Maria, et al. "Building the North Dakota Teaching Force: Insights from the Rural Student Teaching Experience (RSTE)." *Educational Research: Theory and Practice* 37.1 (2026): 20-27.

[30] Delshadi, Amir Mohammad, et al. "Empowerment of Artificial Intelligence (AI) in preventing and detecting ransomware: an analytical review." *Spectrum of Engineering Sciences* (2025): 36-48.

[31] Ahmed, Rana Hassam, et al. "AI-FUZZ: Reinforcement Learning–Guided Stateful Fuzzing for Secure Smart Contracts." *INTERNATIONAL JOURNAL OF ADVANCES IN SIGNAL AND IMAGE SCIENCES* (2025): 1040-1055.

[32] Akram, Muhammad, et al. "Deepfake social engineering attacks: Detection and prevention framework." (2026).

[33] Safiullah, Dilshad, et al. "Machine Learning Applications in Post-Fire Forest Restoration: Current Advances and Future Directions." *Planta Animalia* 5.1 (2026): 309-325.

[34] Zeeshan, Muhammad, et al. "MACHINE LEARNING AND DEEP LEARNING APPROACHES FOR STRENGTHENING CYBER SECURITY IN INTRUSION DETECTION SYSTEM." *Spectrum of Engineering Sciences* (2025): 1274-1286.

[35] Zeeshan, Muhammad, et al. "ENHANCING CYBERSECURITY IN CLOUD COMPUTING USING ZERO TRUST ARCHITECTURE WITH ADAPTIVE RISK-BASED AUTHENTICATION."

[36] Dhasaratha, Chandramohan, et al. "Data privacy model using blockchain reinforcement federated learning approach for scalable internet of medical things." *CAAI Transactions on Intelligence Technology* (2024).

[37] Zhang, Chang, et al. "Anomaly detection and defense techniques in federated learning: a comprehensive review." *Artificial Intelligence Review* 57.6 (2024): 150.

[38] Khraisat, Ansam, et al. "Survey on federated learning for intrusion detection system: Concept, architectures, aggregation strategies, challenges, and future directions." *ACM Computing Surveys* 57.1 (2024): 1-38.

IEER
Institute for Excellence in Education & Research