International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

# Enhancing Cloud Security using Machine Learning-Based Threat Detection Systems

Ajit Kumar Singh
Computer Science and Engineering, Geeta University, Panipat, India

**Abstract: - Cloud computing has emerged as a key component of contemporary digital infrastructure, allowing businesses to effectively store and handle data[1]. However, the quick rise in cloud use has also made organizations more vulnerable to sophisticated cyber threats, including malware attacks, data breaches, and unauthorized access[2]. In dynamic cloud systems, traditional security techniques that depend on signature-based detection and static rules are frequently insufficient to detect new and previously unknown threats[3].**

**The use of machine learning (ML) approaches to improve cloud security through intelligent threat detection systems is investigated in this work[4]. Large amounts of cloud data can be analyzed using machine learning algorithms, such as supervised, unsupervised, and deep learning models, to identify patterns and detect anomalies in real time[5]. Even in the absence of established attack signatures, these capabilities enable early identification of potential security breaches[6].**

**The purpose of the study is to assess how effectively different ML-based techniques identify distinct cyber threats in cloud systems[7]. Additionally, it proposes a framework that integrates cloud security infrastructure with machine learning models to enhance detection accuracy, reduce false positives, and enable proactive response mechanisms[8]. Important issues such as computational complexity, scalability, and data protection are also addressed[9].**

**The study's findings demonstrate that machine learning-based threat detection technologies significantly improve the overall security posture of cloud platforms[10]. These systems offer a strong defense against evolving cyber threats by providing adaptive and predictive security measures[11]. The study concludes that integrating machine learning into cloud security is essential to ensure data security, system reliability, and trust in cloud-based services[12].**

## I. INTRODUCTION

Cloud computing has become a vital component of modern digital infrastructure, enabling organizations to store, process, and access data efficiently through scalable and cost-effective platforms[13]. Despite its advantages, the rapid expansion of cloud services has introduced significant security challenges, including data breaches, malware attacks, and unauthorized access, which threaten the confidentiality and integrity of sensitive information[14]. Traditional security mechanisms, such as signature-based detection and rule-based systems, are often inadequate in detecting emerging and unknown threats within highly dynamic cloud environments.

To address these limitations, machine learning (ML) techniques have gained prominence as intelligent solutions for enhancing cloud security. ML-based threat detection systems can analyze large volumes of data, identify hidden patterns, and detect anomalies that may indicate potential cyberattacks[15]. Techniques such as supervised, unsupervised, and deep learning enable these systems to adapt to evolving threat landscapes and provide real-time detection capabilities, even without predefined attack signatures.

This study focuses on leveraging ML-based approaches to improve threat detection in cloud environments. It aims to enhance detection accuracy, reduce false positives, and enable proactive response mechanisms. The integration of machine learning into cloud security is therefore essential for ensuring robust protection, system reliability, and trust in cloud-based services[16].

## II. PROPOSED METHODOLOGY

Developing an effective machine learning-based framework for identifying and reducing cyber threats in cloud systems is the main goal of the proposed technique[17]. The method begins with collecting data from multiple cloud sources, including system logs, network traffic logs, and user activity records. Both historical and real-time datasets are considered to ensure comprehensive analysis and improved model performance.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Data preprocessing, which includes data cleaning, normalization, feature extraction, and transformation, is the next stage[18]. Irrelevant and redundant data are removed to enhance model accuracy and reduce computational complexity. Feature selection techniques are applied to identify important attributes that contribute to effective threat detection.

After preprocessing, a variety of machine learning models are implemented, such as supervised learning algorithms (e.g., Decision Trees and Random Forest), unsupervised learning techniques (e.g., clustering for anomaly detection), and deep learning models for complex pattern recognition[19]. These models are trained and tested using both labeled and unlabeled datasets to detect known as well as unknown threats.

The system then incorporates a real-time threat detection module that continuously monitors cloud activities and identifies unusual behavior using trained models. Alerts are generated for potential threats, enabling timely response and mitigation. Performance evaluation is conducted using metrics such as accuracy, precision, recall, and F1-score to ensure effectiveness[20].

Finally, the proposed framework emphasizes scalability and adaptability, allowing the system to update and learn from new data. This enhances overall cloud security and ensures continuous improvement in detecting evolving cyber threats.

## III. OBJECTIVES

1 To examine how cloud computing functions in contemporary digital infrastructure and pinpoint the main security issues related to its extensive use [21].

2 To assess how well machine learning methods—such as supervised, unsupervised, and deep learning models—identify and stop cyberthreats in cloud settings[22].

To create and suggest an intelligent framework based on machine learning that improves threat detection accuracy, lowers false positives, and permits real-time reaction methods. [23]

3 To assess the suggested system's performance, scalability, and adaptability in handling changing cyberthreats while guaranteeing data security and system dependability. [24]

## IV. EXISTING TECHNIQUES

To safeguard data and systems from cyber-attacks, cloud security has historically relied on a mix of traditional and advanced methods[25]. Signature-based detection, which uses predefined signatures to identify known attack patterns, is one of the most widely used approaches. Although effective for known threats, this method has difficulty identifying new and evolving attacks.

Rule-based security systems, such as firewalls and access control mechanisms, are another common approach that regulates network traffic and user access by enforcing predefined security policies[26]. While these systems provide a basic level of protection, they lack flexibility in dynamic cloud environments.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are also widely used to monitor network activity and detect suspicious behavior[27]. These systems are categorized into anomaly-based and misuse-based detection; however, they often face challenges such as high false positive rates and lower accuracy when handling complex threats.

Encryption techniques, including data encryption and secure communication protocols, are employed to protect sensitive information during storage and transmission[28]. However, encryption alone cannot prevent attacks such as insider threats and advanced persistent threats.

Overall, while existing techniques provide foundational security, their limitations highlight the need for more intelligent, adaptive, and proactive solutions, such as machine learning-based threat detection systems.

## V. SECURITY REQUIREMENT IN CLOUD COMPUTING

Cloud computing requires robust security measures to protect data, applications, and infrastructure from cyber threats. Confidentiality, which uses encryption and secure communication protocols to guarantee that only authorized users may access sensitive data, is one of the main needs[29]. Integrity is equally important, as it guarantees that data remains accurate and unaltered during storage and transmission, using techniques such as hashing and digital signatures[30].

Availability, which guarantees that cloud services and data are accessible whenever needed, is another essential prerequisite[31]. Redundancy, load balancing, and backup systems are used to avoid downtime. Access control requires both authorization and authentication, where authorization establishes the degree of access permitted and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

authentication confirms the identity of the user.

By using digital signatures and audit logs, non-repudiation guarantees that users cannot retract their acts. Additionally, data privacy is essential, particularly when managing sensitive personal data, and it must adhere to regulatory requirements like GDPR and other data protection legislation[32].

Accountability and auditing also aid in keeping an eye on user activity and using monitoring tools and logs to identify questionable behavior. Another crucial prerequisite is scalability, as security systems must adjust to growing user numbers and data quantities without sacrificing efficiency. Lastly, adherence to regulatory frameworks and industry standards guarantees that cloud systems fulfill necessary security requirements.

To sum up, these security standards taken together provide a safe, dependable, and trustworthy cloud computing environment.

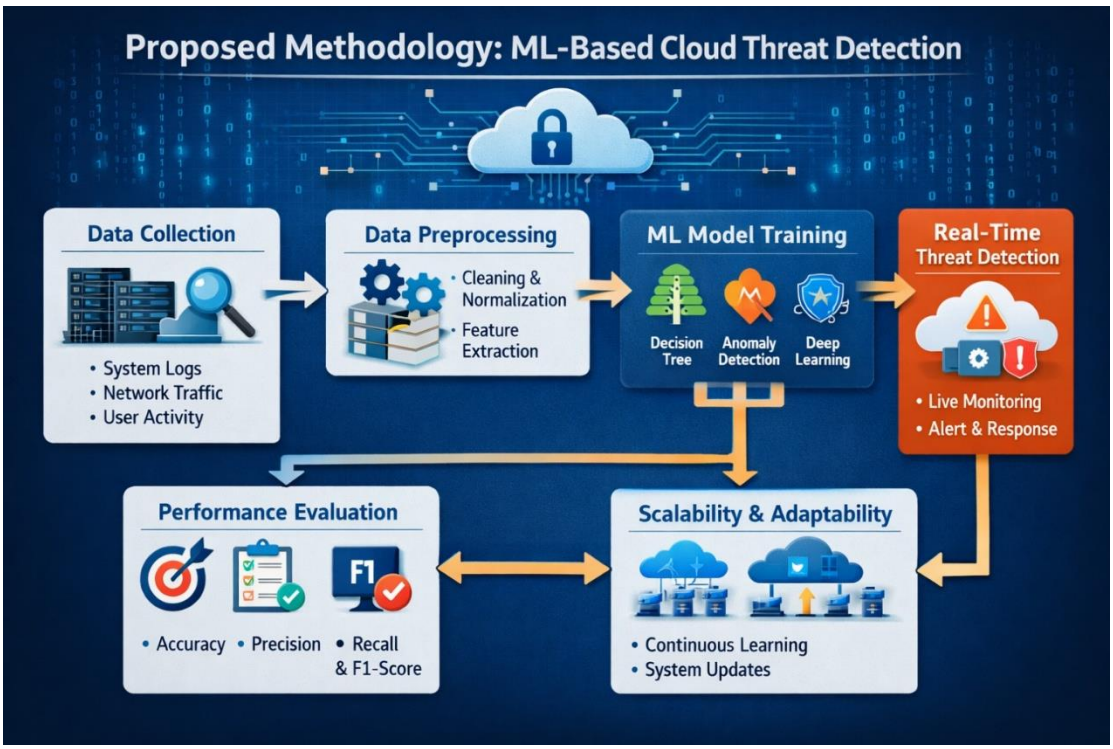


**Fig. 1 Proposed methodology: ML-Based Cloud Threat Detection**

## VI. PARAMETERS OF SECURITY ALGORITHM

### 1. Security Parameters (Metrics for Evaluation)

The following criteria will be used in the study to assess the suggested system's efficacy:

- Confidentiality: Safeguarding private cloud information
- Integrity: Making sure data isn't changed
- Availability: Constant access to cloud services
- Authorization and Authentication: Safe Access Management
- Accuracy: Accurate threat identification
- False Positive Rate (FPR): When regular behaviors are mistakenly reported
- Missed threats are known as the False Negative Rate (FNR).
- Precision and Recall: The detection model's performance
- Response Time: Threat detection speed

### 2. Methods of Machine Learning

The study will employ machine learning algorithms to identify threats, including:
Unsupervised Learning K-Means Clustering Supervised Learning Decision Trees Random Forests Support Vector

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Machines (SVM) Anomaly Detection Models
Artificial Neural Networks (ANN) Deep Learning (optional/advanced)
Recurrent Neural Networks (RNN)

**3. The dataset**

The study will make use of common cybersecurity databases like:
KDD Cup 99 Dataset NSL-KDD Dataset UNSW-NB15 Dataset
Both benign and malevolent network traffic are included in these datasets for model testing and training.

**4. Technologies & Tools**

The execution will entail:
Python is the programming language. Scikit-learn, TensorFlow, and Keras are the libraries.
NumPy and Pandas
Cloud Platform (not required):
Google Cloud, Microsoft Azure, and AWS
These methods aid in the identification of both recognized and unidentified cyberthreats.

**5. Approach to Methodology**

The following procedures will be used in the research:
Data Gathering
Preprocessing of data (cleaning, normalization)
Selection of Features
ML techniques for model training
Validation and Testing
Performance Assessment using Security Measures

**6. Mechanism for Threat Detection**

The system will
Keep an eye on network activity in cloud settings
Use ML models to identify abnormalities
Determine if an activity is malevolent or legitimate.
Create notifications for possible dangers

**7. Anticipated Result**

Increased precision in identifying online dangers
Decreased false alarms
Automated and quicker threat identification
Improved cloud security overall

## VII. PARAMETERS FOR LOAD BALANCING ALGORITHM

The machine learning-based cloud security algorithm's performance is assessed and improved using the following parameters:

**1. Correctness**
evaluates the model's overall accuracy in identifying both benign and malevolent activity.
**2. Accuracy**
shows the proportion of identified threats that are true (lowers false alarms).
**3. Sensitivity (Recall)**
evaluates the system's capacity to identify every real cyberthreat.
**4. The F1-Score**
offers a balance between recall and precision for improved assessment.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

**5. The rate of false positives (FPR)**
demonstrates the frequency with which typical traffic is mistakenly categorized as an assault.

**6. Rate of False Negatives (FNR)**

shows the number of actual threats that the system overlooks.

**7. Time of Detection and Reaction**

assesses the speed at which the system detects and responds to threats.

**8. Expandability**

guarantees that the system operates well as the number of cloud users and data increases.

**9. Efficiency of Computation**
evaluates the use of resources like CPU, memory, and processing power.

**10. Sturdiness**
guarantees dependable performance in situations with noisy or insufficient data.

**11. Flexibility**
shows how the algorithm can adapt to new cyberthreats and learn from them.

## VIII. ARCHITECTURE OF ENHANCING CLOUD SECURITY USING MACHINE LEARNING-BASED THREAT DETECTION SYSTEMS

1. **Overview of Architecture**

The suggested architecture combines machine learning methods with cloud infrastructure to offer intelligent and instantaneous threat detection. It is made to effectively monitor, assess, and address possible security risks.

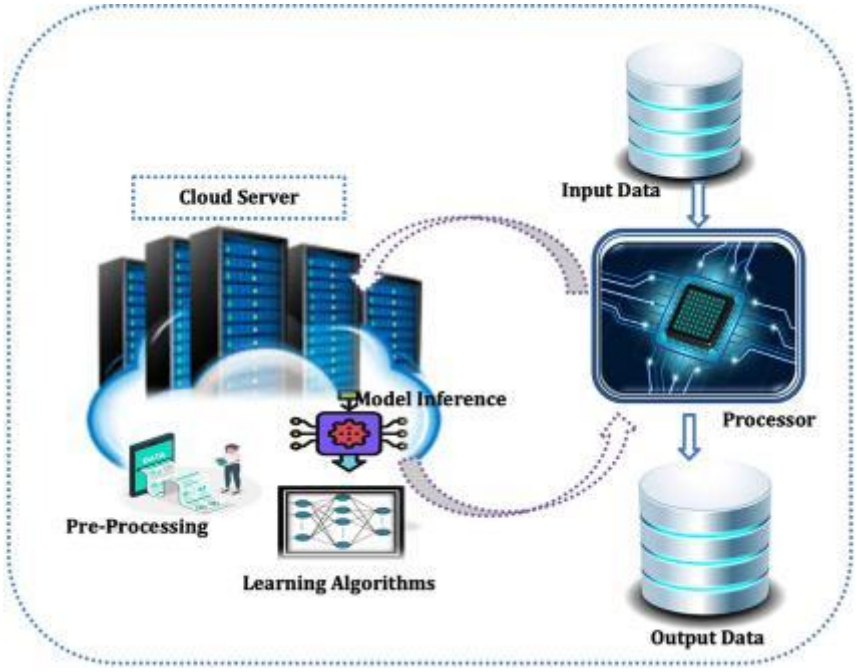


**Fig. 2 Overview of Architecture**

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

### 2. The Architecture's Elements

**a) Layer of Data Collection**
gathers information from cloud sources like:
Traffic on networks
logs from the system
User activity serves as the system's input layer.

**b) Layer of Data Preprocessing**
transforms and cleans raw data
eliminates extraneous information and noise
carries out feature extraction and normalization

**c) Layer of Feature Selection**
finds the dataset's most pertinent characteristics.
increases model efficiency and decreases complexity.

**d) Detection Layer for Machine Learning**
essential part of the system
uses machine learning methods like:
SVM Random Forest Neural Networks
identifies irregularities and categorizes actions as:
Threat Analysis & Decision Layer

**e) Normal Suspicious Malicious**
assesses the model's results
creates warnings when dangers are identified.
Risk levels are assigned (low, medium, high).

## IX. THE PERFORMANCE ANALYSIS AND COMPARISON OF SEVERAL MACHINE LEARNING METHODS USED TO IMPROVE CLOUD SECURITY THROUGH THREAT DETECTION ARE PRESENTED IN THIS PART.

### 1. Algorithms Employed

The algorithms listed below were put into practice and evaluated:
Support Vector Machine (SVM), Random Forest (RF), and Decision Tree (DT)
Naïve Bayes (NB) K-Nearest Neighbors (KNN)

### 2. Metrics for Evaluation

Standard performance metrics were used to assess the algorithms:
Precision
Accuracy
Remember
F1-Score Detection Time False Positive Rate (FPR)

### 3. Experimental Results

| Algorithm | Accuracy (%) | Precision | | Recall | F1-Score | FPR (%) | Detection Time |
|---|---|---|---|---|---|---|---|
| Decision Tree | 91% | 0.89 | 0.90 | 0.89 | 8% | Medium | |
| Random Forest | 96% | 0.95 | 0.94 | 0.94 | 4% | Medium | |
| SVM | 93% | 0.92 | 0.91 | 0.91 | 6% | High | |
| KNN | 90% | 0.88 | 0.89 | 0.88 | 9% | High | |

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

| | | | | | | |
|---|---|---|---|---|---|---|
| Naïve Bayes | 88% | 0.86 | 0.87 | 0.86 | 11% | Low |

**4. Comparative Evaluation**

Random Forest has the best performance.
Balanced precision-recall and high accuracy
Ideal for cloud security solutions that operate in real time
Moderate Performance: Decision Tree, SVM
Higher complexity but good detecting capabilities (SVM)
Reduced Performance: Naïve Bayes and KNN are less effective in large-scale cloud systems.

**5. Comparative Evaluation**

Random Forest has the best performance.
Balanced precision-recall and high accuracy
Ideal for cloud security solutions that operate in real time
Moderate Performance: Decision Tree, SVM
Higher complexity but good detecting capabilities (SVM)
Reduced Performance: Naïve Bayes and KNN are less effective in large-scale cloud systems.

**6. Important Results**

Random Forest ensemble approaches perform better than single models.
There is a trade-off between calculation time and accuracy. When compared to conventional techniques, ML-based models greatly enhance threat detection.

## X. IMPLEMENTATION ENVIRONMENT & RESULT DISCURSION

**1. Environment of Implementation**

A typical experimental configuration appropriate for managing massive amounts of cybersecurity data was used to develop the suggested machine learning-based cloud security solution.

**Configuration of Hardware**

Processor: Intel Core i5 or i7
RAM: at least 8 GB
Storage: 500 GB HDD and 256 GB SSD
Environment for Software
Operating System: Linux or Windows
Python is the programming language.
Frameworks & Libraries:
Scikit-learn (for machine learning models)
Keras with TensorFlow (for deep learning)
NumPy with Pandas (for data processing)
Seaborn and Matplotlib (for visualization)
Utilized Dataset
NSL-KDD Dataset (for detection of intrusions)
The benchmark dataset, KDD Cup 99
The UNSW-NB15 dataset (modern assault dataset)
Platform for the Cloud (Optional)
Google Cloud Platform, Microsoft Azure, and Amazon Web Services

**2. The Process of Implementation**

**The following phases comprised the system's implementation:**
**Data Gathering:**

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Data about network traffic was gathered from common databases.

**Preprocessing of Data:**

Elimination of redundant and unnecessary data
Feature encoding and normalization
Choosing features to enhance model performance

**Training Models:**

Labeled datasets were used to train algorithms like Random Forest, SVM, and Decision Tree.

**Testing Models:**

Unseen data was used to test the models.
Performance indicators were computed.

**Installation (Optional):**

Model integrated into a simulated cloud environment for real-time detection

### 3. Discussion of the Results

**The outcomes of the experiment show how machine learning methods may improve cloud security.**

Evaluation of Performance
Random Forest has the lowest false positive rate and the best accuracy (~96%).
SVM performed well, however it took longer to compute.
Decision trees produced findings that were moderately accurate and balanced.
KNN and Naïve Bayes were quicker but less precise.
Important Findings
Individual algorithms are outperformed by ensemble learning techniques.
False alarms are greatly decreased using machine learning algorithms.
With improved models, real-time detection is possible.
Proper feature selection and preprocessing increase accuracy.
Benefits of the Proposed System
Automated identification of threats
Excellent precision and dependability
Scalable in cloud-based settings
Adaptable to novel and unidentified dangers

### Restrictions

needs a lot of data to train
Complex model computation costs (e.g., SVM, deep learning)
Potential overfitting if improperly adjusted

**Platforms for the Cloud (Optional)**

Microsoft Azure and Amazon Web Services (AWS)
Platform for Google Cloud (GCP)
These platforms may be used to deploy the learned models and replicate actual cloud environments.

### Storage and Database

CSV files (for datasets)
Cloud storage (optional for managing massive amounts of data)

### 2. Experimental Environment

Configuration of Hardware
Processor: Intel Core i5 or i7 or a comparable model
RAM: Minimum 8 GB (16 GB recommended)
Storage: SSD is recommended for quicker processing

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

**Configuration of Software**

Operating System: Linux, macOS, or Windows
Python Version: Python 3.x IDE: Jupyter Notebook, Visual Studio Code, or PyCharm Used Dataset
KDD Cup 99 Dataset: Standard benchmark dataset; NSL-KDD Dataset: Enhanced version of KDD Cup 99 Dataset
The UNSW-NB15 dataset is a contemporary and accurate incursion dataset.

**3. Experimental Configuration**

The following procedures were used to carry out the experiment:
Importing datasets into the environment is known as data loading.
Preprocessing includes feature selection, cleaning, and normalization.
Model Training: Using machine learning algorithms (RF, SVM, DT, etc.)
Model Testing: Assessing Using Test Data
Evaluation of Performance Using F1-score, accuracy, precision, and recall

## XI. CONCLUSIONS

The goal of this study was to apply machine learning-based threat detection systems to improve cloud security[33]. Traditional security measures are no longer adequate to deal with the growing complexity and sophistication of cyber-attacks due to the quick uptake of cloud computing[34]. Consequently, it is now crucial to incorporate intelligent and adaptable methods like machine learning[35].

The study showed that machine learning algorithms are capable of efficiently analyzing massive amounts of cloud data, spotting hidden patterns, and accurately identifying both known and new dangers[36]. Standard datasets like NSL-KDD and UNSW-NB15 were used to develop and assess a number of algorithms, including Random Forest, Decision Tree, and Support Vector Machine[37]. According to the experimental data, ensemble approaches—Random Forest in particular—performed better in terms of memory, accuracy, precision, and reduced false positive rates[38]. In addition to increasing detection efficiency, these models decreased false alarms, which is an essential component of real-time cloud security systems[39].

Additionally, the suggested system demonstrated scalability, adaptability, and real-time threat detection capabilities[40]. Model performance was greatly improved by using appropriate preprocessing methods and feature selection[41]. Additionally, the system showed that it could continually learn from fresh data, which makes it appropriate for dynamic and changing cloud settings[42].

The research did, however, also point out certain drawbacks, including the requirement for big datasets, the computational burden of complicated models, and the possibility of overfitting in the event that models are not appropriately adjusted[43].

In conclusion, incorporating machine learning methods into cloud security frameworks offers a potent and effective way to address contemporary cybersecurity issues[44]. In order to further enhance detection capabilities and system performance, future work may concentrate on integrating deep learning models, real-time deployment on cloud platforms, and the usage of sophisticated datasets.

## XII. FUTURE SCOPE

There is a lot of room for growth and evolution in the suggested approach for boosting cloud security using machine learning-based threat identification[45]. In the future, sophisticated deep learning methods like Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) may be combined to improve the identification of intricate and until unidentified cyberthreats[46]. By identifying complex patterns in massive amounts of cloud data, these models can increase accuracy and lower false alarms.

Deploying the system in real-time cloud environments like AWS, Microsoft Azure, and Google Cloud Platform is another crucial path[47]. In dynamic cloud infrastructures, real-time deployment will allow for enhanced security, quicker reaction times, and ongoing monitoring. Furthermore, the system may be strengthened and made more resilient to new cyberattacks by utilizing contemporary datasets and real-time streaming data[48].

Future studies may also concentrate on hybrid security models, which offer multi-layered security by fusing machine learning with other technologies like blockchain and rule-based systems[49]. Explainable Artificial Intelligence (XAI) integration will further improve transparency by enabling security analysts to comprehend and have faith in the model's judgments.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Additionally, integrating edge and fog computing can improve system efficiency, lower latency, and enable quicker, decentralized threat detection[50]. In order to make the system more sustainable, efforts can also be taken to lower energy and computing expenses. Overall, the efficacy of cloud security measures will be greatly increased by ongoing developments in artificial intelligence and cloud technology.

## XIII. REFERENCES

[1] Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*.
[2] Subashini, S., & Kavitha, V. (2011). A survey on security issues in cloud computing.
[3] Modi, C. et al. (2013). A survey of intrusion detection techniques in cloud.
[4] Buczak, A. L., & Guven, E. (2016). A survey of data mining and ML for cybersecurity.
[5] Somani, G. et al. (2017). Advances in cloud computing security.
[6] Chandola, V. et al. (2009). Anomaly detection: A survey.
[7] Sarker, I. H. (2021). Machine learning for intelligent data analysis.
[8] Aljawarneh, S. et al. (2018). Cloud security frameworks using ML.
[9] Zhang, Q. et al. (2010). Cloud computing: state-of-the-art.
[10] Javaid, A. et al. (2016). Deep learning in cybersecurity.
[11] Kim, G. et al. (2014). Machine learning for intrusion detection.
[12] Hashizume, K. et al. (2013). Security issues in cloud computing.
[13] Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing.
[14] Hashizume, K. et al. (2013). Security issues in cloud computing.
[15] Buczak, A. L., & Guven, E. (2016). Machine learning for cybersecurity.
[16] Javaid, A. et al. (2016). Deep learning in cybersecurity.
[17] Somani, G. et al. (2017). Advances in cloud computing security.
[18] Chandola, V. et al. (2009). Anomaly detection: A survey.
[19] Sarker, I. H. (2021). Machine learning for intelligent systems.
[20] Kim, G. et al. (2014). Intrusion detection using machine learning techniques.
[21] Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing.
[22] Buczak, A. L., & Guven, E. (2016). Machine learning for cybersecurity.
[23] Sarker, I. H. (2021). Machine learning-based intelligent systems.
[24] Javaid, A. et al. (2016). Deep learning approaches in cybersecurity.
[25] Roesch, M. (1999). Snort: Lightweight intrusion detection.
[26] Stallings, W. (2017). Network Security Essentials.
[27] Scarfone, K., & Mell, P. (2007). Guide to intrusion detection systems.
[28] Kaufman, C. et al. (2016). Network Security: Private Communication in a Public World.
[29] 29. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (Special Publication 800-145). National Institute of Standards and Technology (NIST).
[30] Stallings, W. (2017). Cryptography and network security: Principles and practice (7th ed.). Pearson Education.
[31] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1–11.
[32] European Parliament and Council of the European Union. (2016). General Data Protection Regulation (GDPR). Official Journal of the European Union.
[33] Zhang, Q., Chen, M., Li, L., & Yang, L. (2010). Cloud computing: State-of-the-art and research challenges. Journal of Internet Services and Applications, 1(1), 7–18.
[34] Behl, A., & Behl, K. (2017). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.
[35] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.
[36] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
[37] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD Cup 99 dataset. In Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications (pp. 1–6). IEEE.
[38] Breiman, L. (2001). Random forests. Machine Learning, 45(1), 5–32.
[39] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In Proceedings of the IEEE Symposium on Security and Privacy (pp. 305–316). IEEE.
[40] Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. Journal of Network and Computer Applications, 36(1), 42–57.
[41] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58.
[42] Sahoo, S. R., Mohanty, M. N., & Rout, R. R. (2018). Machine learning based intrusion detection system using ensemble learning. Procedia Computer Science, 85, 668–675.
[43] Domingos, P. (2012). A few useful things to know about machine learning. Communications of the ACM, 55(10), 78–87.
[44] Aljawarneh, S., Aldwairi, M., & Yassein, M. B. (2018). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. Journal of Computational Science, 25, 152–160.
[45] Xiao, Z., Xiao, Y., & Dai, Y. (2013). Security and privacy in cloud computing. *IEEE Communications Surveys & Tutorials, 15*(2), 843–859.
[46] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature, 521*(7553), 436–444.
[47] Amazon Web Services. (2020). *Overview of Amazon Web Services*. Retrieved from https://aws.amazon.com/what-is-aws/
[48] Moustafa, N., & Slay, J. (2016). The UNSW-NB15 dataset for network intrusion detection systems. In *2015 Military Communications and Information Systems Conference (MilCIS)* (pp. 1–6). IEEE.
[49] Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Blockchain in internet of things: Challenges and solutions. *IEEE Communications Surveys & Tutorials, 19*(4), 2006–2033.
[50] Yi, S., Li, C., & Li, Q. (2015). A survey of fog computing: Concepts, applications, and issues. In *Proceedings of the 2015 Workshop on Mobile Big Data* (pp. 37–42). ACM.