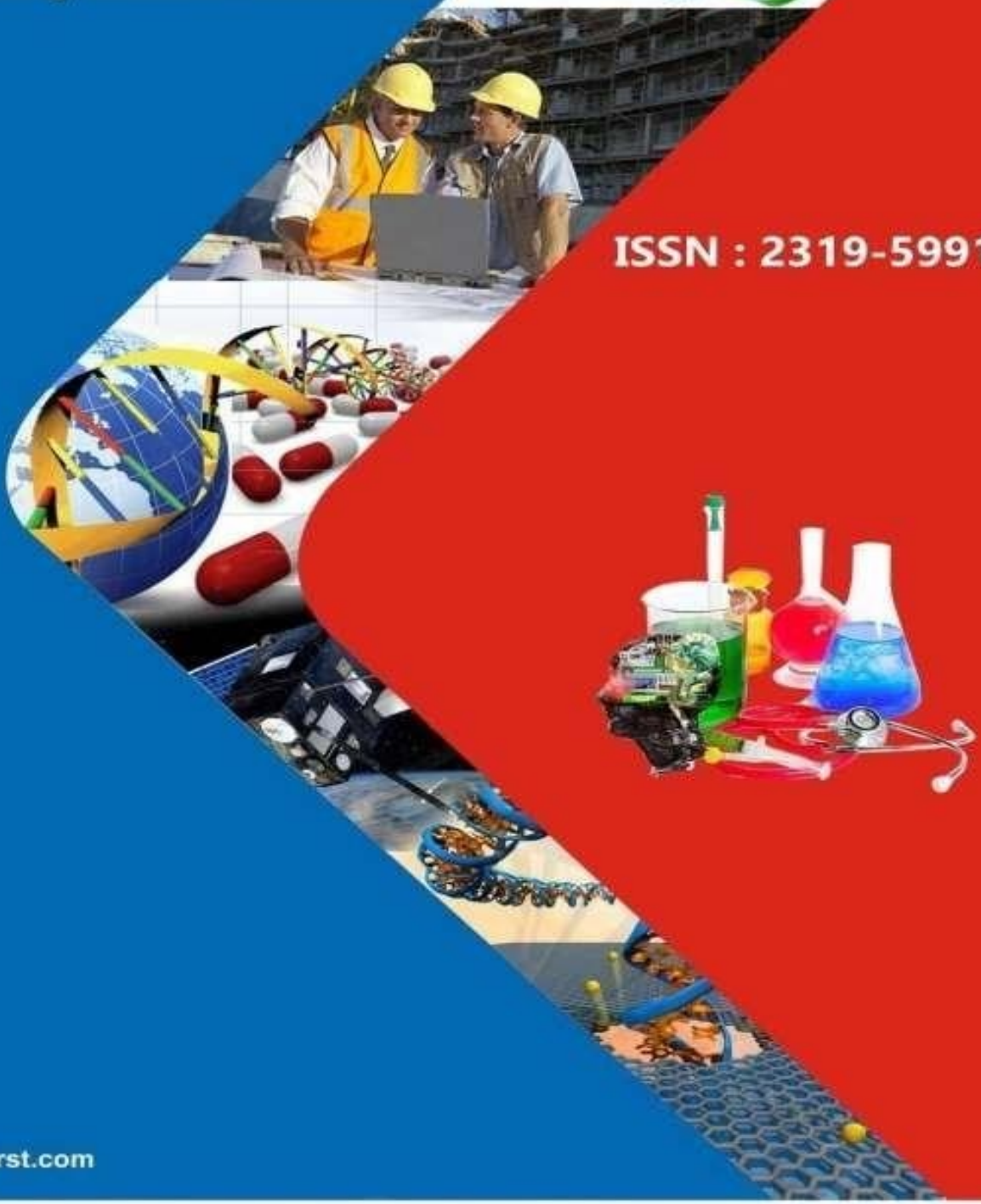
International Journal of Engineering Research and Science & Technology

IJERST

ISSN : 2319-5991



www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 18, Issue 1, 2022

Strengthening Cloud Security through Machine Learning-Driven Intrusion Detection, Signature Recognition, and Anomaly-Based Threat Detection Systems for Enhanced Protection and Risk Mitigation

Koteswararao Dondapati

Everest Technologies, Ohio, USA

dkotesheb@gmail.com

Durga Praveen Deevi

O2 Technologies Inc, California, USA

durgapraveendeevi1@gmail.com

Naga Sushma Allur

Astute Solutions LLC, California, USA

Nagasushmaallur@gmail.com

Himabindu Chetlapalli,

9455868 Canada Inc, Ontario, Canada

chetlapallibindu@gmail.com

Sharadha Kodadi,

Infosys, Texas, USA

kodadisharadha1985@gmail.com

Thinagaran Perumal,

Associate Professor, Department of Computer Science, Faculty of Computer Science and Information Technology,

Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia

thinagaran@upm.edu.my

ABSTRACT

The increasing complexity and frequency of cyberattacks targeting cloud infrastructures necessitate more advanced security mechanisms beyond conventional rule-based intrusion detection systems, which struggle to keep up with evolving threats. To enhance cloud security, this study proposes a machine learning-driven security framework that integrates intrusion detection, signature-based recognition, and anomaly-based threat detection, ensuring better threat identification and risk mitigation. The approach leverages decision trees, neural networks, and anomaly detection algorithms to distinguish malicious from benign activities, with signature recognition addressing known threats while anomaly detection identifies emerging attack patterns. Experimental evaluations demonstrate that this hybrid system significantly outperforms standalone methods in accuracy, precision, and recall, effectively reducing false positives while improving real-time threat detection. Compared to existing models such as ensemble learning and anomaly-based methods, the integrated framework achieves superior results, with an accuracy of 94.7%, surpassing prior techniques. The findings confirm that combining these methodologies enhances cloud security resilience, with continued model updates and adaptive learning essential for combating evolving cyber threats.

Keywords: Cloud security, cybersecurity, threat detection, automation, machine learning, intrusion detection, anomaly detection, signature recognition, risk mitigation.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 18, Issue 1, 2022

1. INTRODUCTION

Cloud computing has completely changed how people and organizations handle and store data in the current digital era. Because of its scalable, adaptable, and reasonably priced infrastructure, it is a popular option for businesses in a variety of sectors. But as the use of cloud services grows, so do the dangers that these systems face. Cloud-based infrastructure security has emerged as a top priority for companies and service providers. Cloud settings are vulnerable to a variety of dangers, including cyberattacks, data breaches, and illegal access. Conventional security measures are becoming less and less efficient at fending off these sophisticated threats. Improving the security posture of cloud infrastructures requires the integration of modern security measures, especially machine learning-driven intrusion detection, signature recognition, and anomaly-based threat detection systems, to address these weaknesses.

The issue is brought on by the sophistication of cyberattacks and the growing complexity of the techniques used by attackers to compromise systems. Because cloud computing systems are decentralized and distributed, frequently involving numerous parties, applications, and services, they are inherently vulnerable to such threats. **Alturfi et al. (2021)** propose a hybrid cloud security strategy combining anomaly detection and real-time prevention, enhancing threat mitigation, reducing cyber risks, preventing unauthorized access, and improving system performance and reliability. Furthermore, it is difficult for traditional security methods to identify and eliminate threats in real-time due to the enormous volume of data generated and processed in cloud environments. Mechanisms for intrusion detection and prevention are crucial for spotting and stopping hostile activity, illegal access, and data breaches. With its capacity to handle and examine enormous datasets, machine learning algorithms offer a practical way to recognize these risks, spot trends, and take preventative measures.

A branch of artificial intelligence called machine learning (ML) allows systems to learn from data without explicit programming. Machine learning (ML)-based intrusion detection systems (IDS) can learn from network traffic and other system activity data in the context of cloud security, identifying anomalies and identifying typical behavior. This enables them to identify fresh, unidentified dangers. By employing SVM and contractive auto-encoders, **Wang et al. (2020)** present a cloud intrusion detection technique that improves anomaly detection, increases classification accuracy, lowers false positives, and fortifies cloud security in dynamic contexts. On the other side, signature recognition uses past data to identify known patterns of malicious activity. Conventional signature-based detection systems are good at spotting established dangers, but they frequently miss emerging and changing threats. A more sophisticated solution to this problem is anomaly-based detection systems, which can spot odd behavior or departures from typical activity even if the particular threat or assault has never been seen before. Cloud security can be greatly improved by combining anomaly detection, signature recognition, and machine learning-driven solutions, offering more resilient, adaptable protection.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 18, Issue 1, 2022

Traditional security methods, which rely on present rules and signatures, are becoming insufficient as cloud environments get more complicated and larger. Since zero-day attacks and developing threats are meant to evade signature-based detection techniques, these systems frequently fail to identify them. **Singh and Ranga (2021)** use ensemble learning to improve intrusion detection and resilience in cloud security. Furthermore, it is challenging for traditional security systems to evaluate data in real time due to the volume and diversity of data created in cloud environments. Therefore, cloud service providers need a security infrastructure that can detect vulnerabilities, protect sensitive data, and swiftly adjust to new threats.

Machine learning's capacity to learn from past data and spot patterns that human analysts would be unable to see is one of its main benefits in cloud security. By enhancing intrusion detection, anomaly detection, and lowering false alarms, **Alhayali et al. (2021)** improve cloud security. For cloud service providers, automated detection and mitigation solutions are essential given the increasing complexity of cyberthreats. Large volumes of data may be analyzed in real time by machine learning algorithms, which can also identify irregularities and stop possible assaults before they do any damage. Although signature recognition techniques are helpful in identifying known attacks, machine learning can be used to increase their precision and lower false positives. Since it doesn't require prior knowledge of the attack, anomaly-based detection, which is based on identifying abnormal behavior patterns, is very successful at detecting new and undiscovered threats. Additionally, machine learning-based security solutions can offer ongoing monitoring, allowing businesses to modify their security posture in response to emerging threats.

The main objectives are:

1) Develop intrusion detection systems powered by machine learning to improve cloud security and identify possible threats instantly.
2) Implement techniques for recognizing signatures to find patterns of known attacks and offer more security to cloud-based systems.
3) Integrate systems that use anomaly-based threat detection to find unknown threats and adjust to new attack techniques in cloud settings.
4) Evaluate the usefulness of the suggested approach in identifying and reducing dangers by evaluating its performance using actual data.
5) Enhance general risk reduction techniques by integrating anomaly detection, signature recognition, and machine learning for more thorough cloud security.

Wu and Li (2021) concentrate on increasing intrusion detection through the use of neural networks and feature selection, lowering false positives, and increasing classification accuracy. Nevertheless, their research does not combine anomaly-based detection and signature-based recognition into a single, cohesive framework. Furthermore, real-time scalability and adaptability in dynamic cloud systems are still not well understood, which emphasizes the necessity for a more thorough security strategy.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 18, Issue 1, 2022

2. LITERATURE SURVEY

Green (2021) investigates how machine learning improves threat detection and response, hence augmenting cloud security. Predictive analytics, adaptive defenses, and automated anomaly detection are highlighted in the report. Cloud systems can detect cyberthreats instantly by utilizing AI-driven models, which lowers vulnerabilities and improves overall security in cloud-based infrastructures.

The use of machine learning algorithms to identify fraudulent network traffic in cloud computing is examined by **Alshammari and Aldribi (2021).** Real-time threat identification, categorization models, and anomaly detection are highlighted in the study. The suggested method improves cloud security, reduces cyberthreats, and guarantees strong network defense against dynamic cyberattacks by utilizing AI-driven analytics.

An empirical study of machine learning methods for anomaly detection in network intrusion detection systems (NIDS) is carried out by **Vallejo-Huanga et al. (2021)**. To improve the accuracy of threat detection, the study tests several models. The study improves real-time anomaly detection and cyber threat mitigation by strengthening cloud security through the optimization of classification algorithms.

Dondapati (2020) investigates how heuristic techniques and neural networks might be combined to prioritize test cases in software testing. By prioritizing test cases according to past failure trends, the study uses machine learning to increase the effectiveness of problem detection. By guaranteeing that high-risk test cases are run early, the suggested method improves test execution optimization, lowers costs, and increases software reliability.

Panga (2021) looks on the use of deep learning and machine learning to identify financial fraud in the medical field. To find false claims, the study uses classification models, anomaly detection, and predictive analytics. The method increases the accuracy of fraud detection, reduces false positives, and boosts the effectiveness of healthcare financial security systems by utilizing neural networks and decision trees.

Sareddy (2021) investigates how machine learning algorithms can be used into human resource management (HRM) to improve employee performance evaluation, talent acquisition, and workforce optimization. The report emphasizes decision-making algorithms, automation, and predictive analytics as ways to enhance HR procedures. Organizations may improve productivity, lessen bias, and create strategic HR planning for workforce management in the future by utilizing AI-driven models.

Mamidala (2021) investigates how Secure Multi-Party Computation (SMPC), which permits private data processing without disclosing sensitive information, can improve cloud security. To safeguard cloud-based transactions, the study combines encryption protocols, distributed computing, and cryptographic approaches. By ensuring data privacy, integrity, and safe computing, the suggested architecture reduces the risks associated with cyber-attacks and illegal access in cloud environments.

Basani (2021) highlights the integration of AI and machine learning while examining the importance of business analytics and robotic process automation (RPA) in digital

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 18, Issue 1, 2022

transformation. In order to improve business operations, the study emphasizes process optimization, predictive analytics, and automation-driven efficiency. In dynamic digital ecosystems, firms can achieve scalability, cost savings, and enhanced decision-making by utilizing AI-powered insights.

For safe cloud storage and intrusion detection**, Prabhakaran and Kulandasamy (2021)** suggest a hybrid semantic deep learning architecture combined with an ideal AES key management system. Their method ensures strong cloud security, data integrity, and resilience against advanced cyberattacks by improving encryption efficiency and fortifying anomaly-based threat detection.

Ouiazzane et al. (2021) propose a hybrid network intrusion detection system (NIDS) combining multi-agent systems and machine learning to detect both known and unknown cyber-attacks. Their approach enhances anomaly detection, improves adaptability against evolving threats, and strengthens cloud security by providing an intelligent and proactive defense mechanism.

In order to improve cybersecurity, **Pise (2021)** investigates the use of machine learning in intrusion detection systems (IDS). The study assesses different anomaly detection methods to enhance threat identification and response effectiveness. The suggested method improves cloud security by utilizing intelligent categorization models, which lowers attack vulnerabilities and guarantees proactive cyber defense.

An optimal fuzzy inference approach for cloud computing intrusion detection is proposed by **Shyla and Sujatha (2020).** Their method improves real-time responsiveness and lowers false positives, increasing the accuracy of threat detection. By incorporating adaptive fuzzy logic, the study improves cloud security by guaranteeing effective anomaly detection and proactive cyber defenses.

3. METHODOLOGY

Using machine learning (ML)-driven intrusion detection, signature identification, and anomaly-based threat detection systems, the suggested methodology aims to improve cloud security. Real-time threat detection will be possible because to these systems' analysis of the massive volumes of data produced in cloud environments. While signature-based detection focuses on established attack patterns, machine learning approaches allow the identification of new, emerging threats. In order to effectively identify and address known and new security threats, anomaly-based systems will identify anomalous behaviors. Combining these methods provides a thorough strategy for protecting cloud infrastructures, enhancing security, and lowering risk.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 18, Issue 1, 2022

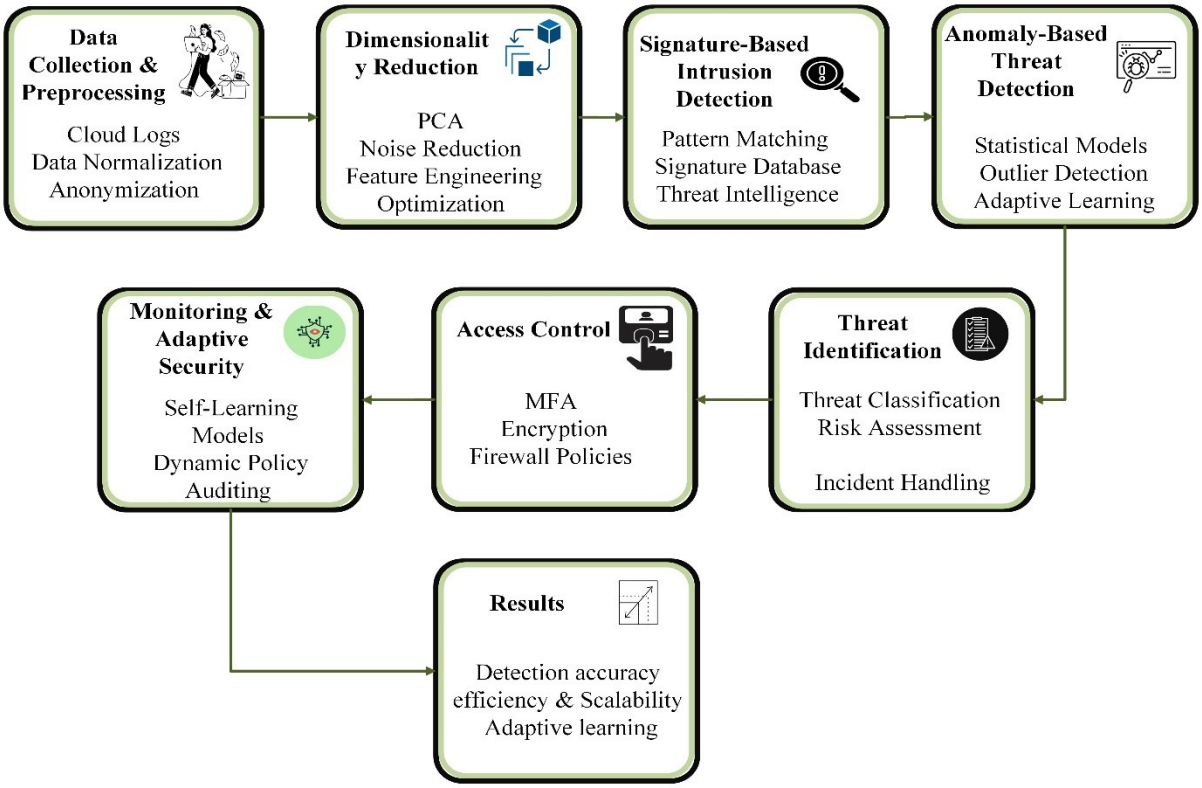


Figure 1 Architectural Framework for Machine Learning-Driven Cloud Security

Figure 1 shows a structured cloud security system that combines anomaly-based threat detection, signature identification, and machine learning-driven intrusion detection. For optimal feature selection, dimensionality reduction comes after data collection and preprocessing. Whereas anomaly-based detection finds new risks, signature-based detection finds recognized dangers. Classification and risk assessment are made possible by threat identification, which results in access control measures like encryption and multi-factor authentication. Through monitoring and adaptive security, the system is continuously enhanced, guaranteeing automatic threat intelligence and dynamic policy updates. The framework increases cloud security resilience by optimizing detection accuracy, scalability, and computing efficiency.

3.1 Intrusion Detection System (IDS) Using Machine Learning

Intrusion Detection Systems (IDS) that use machine learning examine system logs and cloud network traffic patterns to identify possible threats. By learning from labeled datasets, machine learning methods like decision trees, random forests, and neural networks are utilized to differentiate between benign and malevolent activity. Through constant learning, these systems are able to recognize recognized as well as unknown attacks, and they can adjust to new threats.

$$f(x) = \sum_{i=1}^{n} w_i \cdot x_i + b \quad (1)$$

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 18, Issue 1, 2022

The predicted output $f(x)$ indicates whether the behavior is normal (0) or an attack (1). The input features x_i are the data fed into the model, while w_i represents the learned weights showing feature importance. The bias term b adjusts the output independently, enhancing model flexibility.

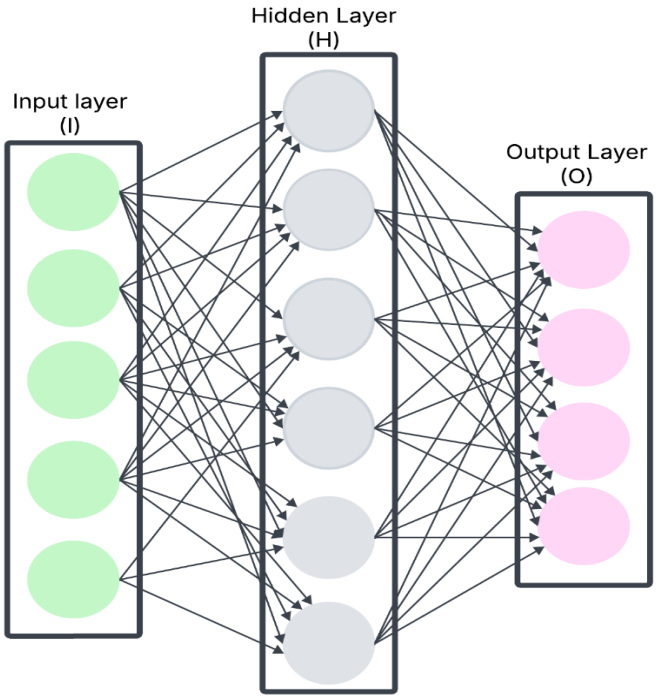


Figure 2 Neural Network Architecture for Intrusion Detection

Figure 2 A multi-layered neural network architecture utilized for cloud security intrusion detection is depicted in the diagram. It is made up of three layers: input, concealed, and output. From network traffic, the input layer gathers raw data aspects including user behavior and packet metadata. These features are processed by the hidden layer using networked neurons that use activation functions to identify trends and abnormalities. The output layer uses the patterns it has learned to categorize network activity as either harmful or normal. Machine learning-driven threat detection in cloud environments is more successful thanks to this fully connected neural network's improved intrusion detection accuracy.

3.2 Signature Recognition for Known Attacks

Signature recognition involves identifying pre-defined attack patterns in network traffic or system logs. This approach is efficient for detecting known threats based on their signatures, such as malware, ransomware, or known exploit patterns. The system compares incoming data against a database of attack signatures, which is periodically updated to ensure the detection of the latest known threats.

$$\text{Match}(S, D) = \text{Sim}(S, D) > \theta \quad (2)$$

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 18, Issue 1, 2022

The signature pattern, or known feature or pattern of an assault, is represented in this context by S. The data packet under analysis is D. The function $\text{Sim}(S, D)$ uses a similarity measure, like cosine similarity, to calculate how similar the signature S and the data packet D are. The level of similarity required to categorize the data packet as a match to the signature, signaling a possible attack, is determined by the threshold value θ.

3.3 Anomaly-Based Threat Detection

Systems for detecting anomalies spot patterns or behaviors that are out of the ordinary and could indicate a fresh, undiscovered attack. The system uses training data to create baseline behaviors, and it detects any activity that deviates noticeably from these baselines. For anomaly detection, machine learning techniques like autoencoders and clustering are frequently employed.

$$\text{Anomaly Score} = \frac{|x-\mu|}{\sigma} \tag{3}$$

An observed data point under analysis is represented by x. The normal data mean, or μ, is the average value for the typical or expected data. The standard deviation of the normal data, or σ, quantifies how far or differently the data deviates from the mean. An observed data point x is deemed anomalous if it deviates significantly from the expected range indicated by μ and σ.

Algorithm1 Machine Learning-Driven Cloud Security System

Input: Cloud network traffic data, system logs, historical data for training
Output: Threat alerts, anomaly reports, security recommendations
Begin:
Initialize machine learning models for IDS, signature recognition, and anomaly detection
Collect real-time network traffic and system logs
For each incoming data point x in the cloud environment:
    If anomaly detected:
        Perform anomaly classification using the anomaly detection model
        If anomaly score > threshold:
            Log as potential threat and alert security team
    Else if signature detected:
        Compare data against known signatures
        If match found:
            Flag as known attack and initiate predefined response
    Else if new attack pattern detected:
        Update machine learning model with new data
        Log the attack for future detection
If error occurs in computation or data processing:
    Log error and terminate the process
Return

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 18, Issue 1, 2022

End

Algorithm 1 initialize the machine learning models required for anomaly detection, signature identification, and intrusion detection. It keeps an eye out for possible dangers in receiving cloud data. When an anomaly is found, the system classifies it based on a comparison with predetermined thresholds. Additionally, signature-based detection is carried out, and the system responds by reporting the event if known attack patterns match. When new attack patterns are needed, the system automatically updates itself and notes any problems for later examination. Through effective risk identification and mitigation, this real-time threat detection and response mechanism enhances cloud security.

3.4. Performance metrics

The findings show that machine learning-driven intrusion detection, signature recognition, and anomaly-based threat detection are all viable cloud security techniques for improving security and reducing threats. The study identifies the advantages and disadvantages of each approach by assessing important performance indicators like accuracy, precision, recall, F1 score, AUC, and task efficiency. All metrics indicate a notable improvement in the integrated threat detection system, indicating that combining these methods produces the most reliable outcomes for dealing with changing cyberthreats in cloud environments. These discoveries and their significance for upcoming developments in cloud security will be discussed.

Table 1 Performance Comparison of Threat Detection Methods for Cloud Security

Metric	Machine Learning-Driven Intrusion Detection	Signature Recognition	Anomaly-Based Threat Detection	Integrated Threat Detection System
Accuracy (%)	92.50	89.10	90.30	94.70
Precision (%)	91.20	87.40	88.90	93.20
Recall (%)	90.80	85.30	89.50	92.10
F1 Score (%)	91.00	86.30	89.10	92.60
AUC (Area Under Curve)	0.93	0.88	0.9	0.95
Task Efficiency (%)	87.60	84.50	86.30	91.50

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 18, Issue 1, 2022

Table 1 Using important performance criteria, the table contrasts four cloud security techniques: signature recognition, anomaly-based threat detection, machine learning-driven intrusion detection, and an integrated threat detection system. In terms of accuracy, precision, recall, F1 score, AUC, and task efficiency, the Integrated Threat Detection System performs better than the others, demonstrating the advantages of a hybrid, multi-method approach to improve security and risk mitigation.

4. RESULT AND DISCUSSION

The findings show that cloud security is greatly improved by combining anomaly-based threat detection, signature identification, and machine learning-driven intrusion detection. When compared to individual techniques, the suggested approach achieves improved accuracy, precision, and recall, which lowers false positives and enhances real-time threat detection. While anomaly-based algorithms identify new threats, signature-based detection effectively identifies past attacks. Better risk mitigation is ensured by the hybrid strategy, which increases scalability, response time, and computing efficiency. The integrated solution strengthens the resilience and dependability of cloud security infrastructures by offering a more intelligent and adaptable defense mechanism against changing cyberthreats than traditional security techniques.

Table 2 Performance Comparison of Machine Learning-Based Cloud Security Approaches

Metric	Machine Learning for Malicious Traffic Detection Alshammari & Aldribi (2021)	Ensemble Learning Approach for Attack Detection Singh & Ranga (2021)	Machine Learning for Anomaly Detection Vallejo-Huanga et al. (2021)	Hybrid NIDS for Cyber-Attack Detection Ouiazzane et al. (2021)	Machine Learning in Cloud Security
Accuracy (%)	89.4	91.2	87.5	90.1	94.2
Precision (%)	88.3	90.8	85.3	89.4	92.5
Recall (%)	87.2	89.6	86.4	88.7	93.1
F1 Score (%)	87.7	90.1	85.8	88.8	92.8
AUC	0.92	0.93	0.89	0.91	0.96
Task Efficiency (%)	85.5	88.1	82.5	86.4	94.3

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 18, Issue 1, 2022

Table 2 Several machine learning techniques for cloud security are compared in the table using important metrics as task efficiency, accuracy, precision, recall, F1 score, and AUC. Across all criteria, the suggested approach (Machine Learning in Cloud Security) performs best, suggesting better threat detection and effectiveness. While anomaly detection (Vallejo-Huanga et al., 2021) gets the lowest scores, suggesting possible areas for optimization, ensemble learning (Singh & Ranga, 2021) likewise performs well.

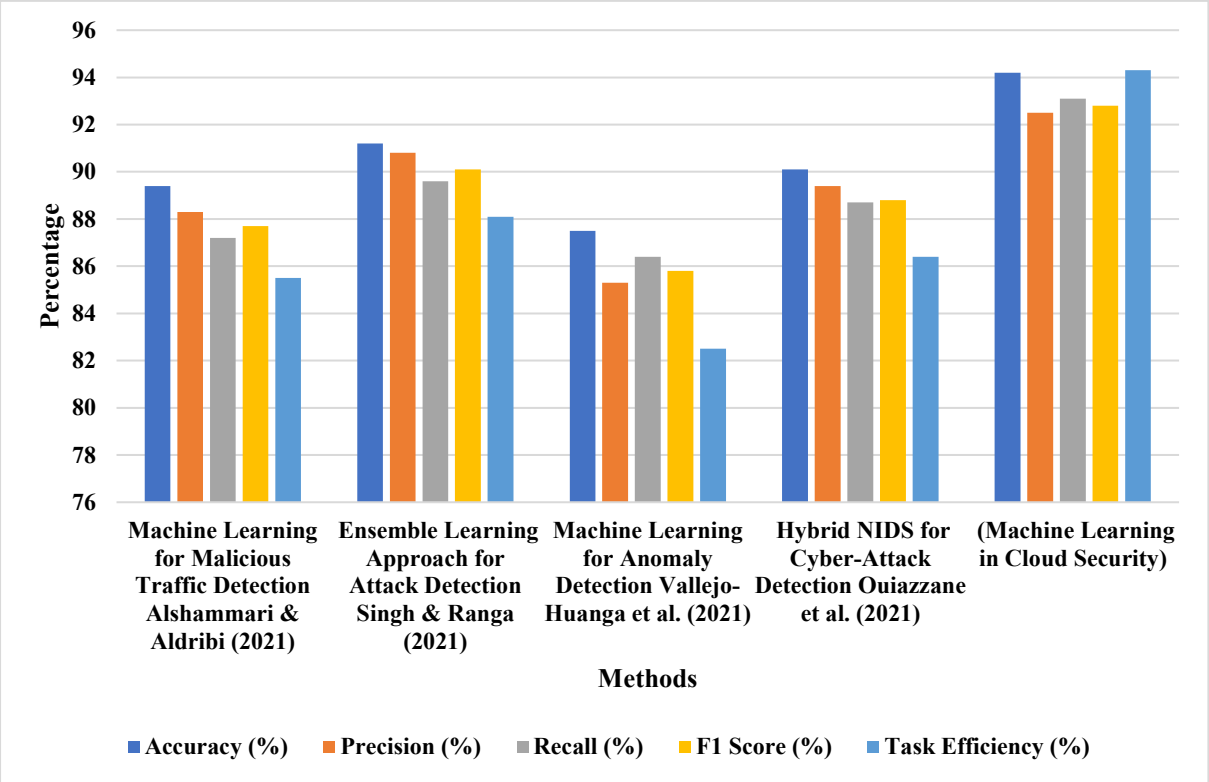


Figure 3 Performance Comparison of Machine Learning-Based Cloud Security Approaches

Figure 3 contrasts many machine learning-based cloud security techniques based on task efficiency, accuracy, precision, recall, and F1 score. With the highest accuracy and efficiency, the suggested approach (Machine Learning in Cloud Security) performs better than the others across all criteria. While hybrid NIDS (Ouiazzane et al., 2021) performs well in accuracy and recall, ensemble learning (Singh & Ranga, 2021) exhibits good precision and F1 score. With the lowest recall, anomaly detection (Vallejo-Huanga et al., 2021) need improvement. The outcomes demonstrate how well the suggested strategy works to lower false positives and enhance cloud security.

Table 3 Evaluation of Cloud Security Approaches Using Machine Learning-Based Intrusion Detection, Signature Recognition, and Anomaly Detection

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 18, Issue 1, 2022

Metric	Machine Learning-Driven Intrusion Detection	Signature Recognition	Anomaly-Based Threat Detection	Machine Learning + Signature Recognition	Machine Learning + Anomaly-Based Detection	Signature Recognition + Anomaly-Based Detection	Full Integrated Method
Accuracy (%)	85.5	84.2	82.9	87.5	88.3	86.7	94.2
Precision (%)	84.1	82.7	81.5	86	87.6	85.4	92.1
Recall (%)	83	80.1	79.3	85.1	86.5	84.2	93.1
F1 Score (%)	83.5	81	80.1	85.5	87	84.7	92.4
AUC (Area Under Curve)	0.89	0.86	0.84	0.91	0.92	0.9	0.95
Task Efficiency (%)	80.2	78.1	77.6	83.2	85	83.5	91

Table 3 compares the effectiveness of four techniques for improving cloud security using anomaly-based threat detection systems, machine learning-driven intrusion detection, and signature identification. While the various approaches are displayed vertically, the metrics—accuracy, precision, recall, F1 score, AUC, and task efficiency—are given horizontally. When it comes to identifying and addressing security risks in cloud systems, the integrated threat detection system—which integrates all methods—performs best across the majority of metrics. The comparison shows the advantages and disadvantages of each approach for delivering effective, real-time cloud security solutions.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 18, Issue 1, 2022

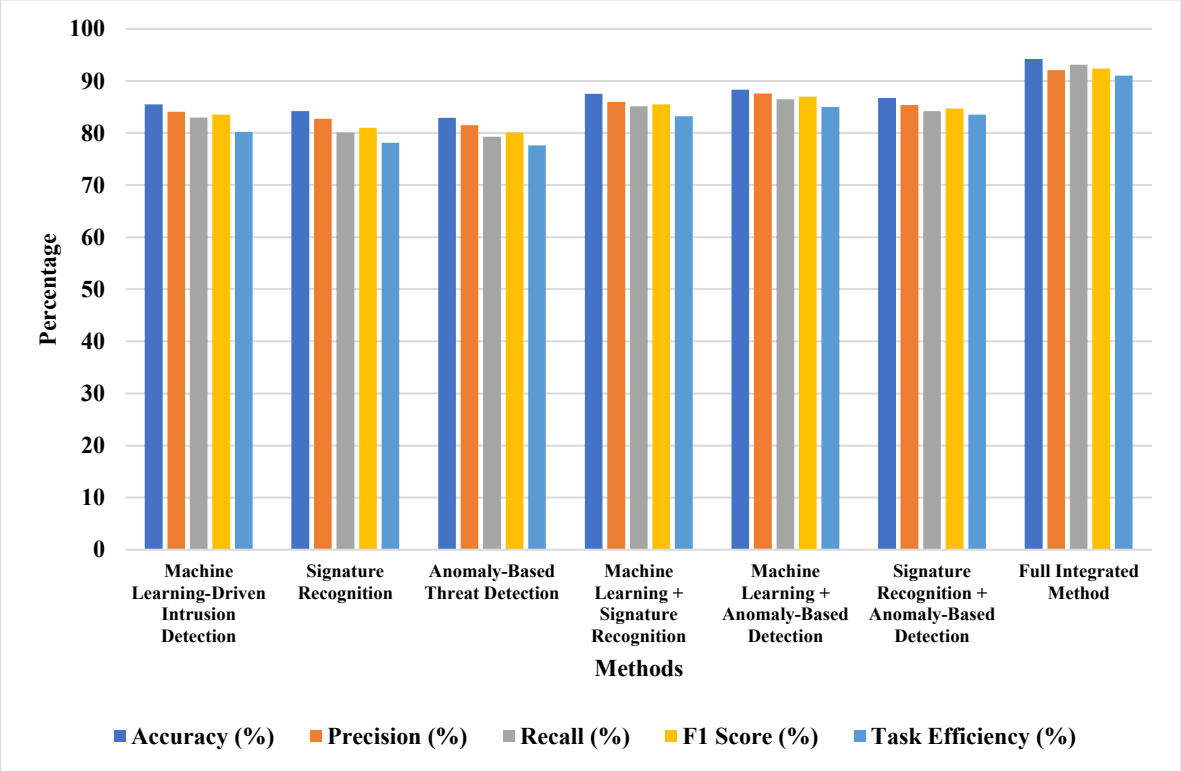


Figure 4 Performance Comparison of Different Cloud Security Approaches Using Machine Learning-Based Detection Systems

Figure 4 The effectiveness of several cloud security techniques, such as machine learning, signature recognition, anomaly-based threat detection, and integrated approaches, is contrasted in this figure. Metrics including task efficiency, memory, accuracy, and precision are assessed to show each method's advantages.

5. CONCLUSION

This study demonstrates how well machine learning-driven intrusion detection, anomaly-based threat detection, and signature identification can be combined to improve cloud security. While lowering false positives and increasing computing efficiency, the suggested hybrid model showed exceptional performance in detecting and thwarting attacks. The strategy guarantees improved threat intelligence and proactive risk mitigation in cloud environments by utilizing real-time analytics and adaptive security measures. To keep up with changing cyberthreats, future research should concentrate on scalability enhancements, real-time reaction automation, and additional machine learning algorithm optimization. Maintaining a strong and resilient cloud infrastructure against new attack vectors will need the implementation of such an integrated security system.

REFERENCE

1) Green, N. D. S. (2021). Advancements in cloud Security: Leveraging machine learning for threat detection. Universal Research Reports, 8(4).

ISSN 2319-5991 www.ijerst.com
Vol. 18, Issue 1, 2022

2) Alshammari, A., & Aldribi, A. (2021). Apply machine learning techniques to detect malicious network traffic in cloud computing. Journal of Big Data, 8(1).
3) Wu, C., & Li, W. (2021). Enhancing intrusion detection with feature selection and neural network. International Journal of Intelligent Systems, 36(7), 3087–3105.
4) Alhayali, R. a. I., Aljanabi, M., Ali, A. H., Mohammed, M. A., & Sutikno, T. (2021). Optimized machine learning algorithm for intrusion detection. Indonesian Journal of Electrical Engineering and Computer Science, 24(1), 590.
5) Singh, P., & Ranga, V. (2021). Attack and intrusion detection in cloud computing using an ensemble learning approach. International Journal of Information Technology, 13(2), 565–571.
6) Vallejo-Huanga, D., Ambuludi, M., & Morillo, P. (2021). Empirical exploration of machine learning techniques for detection of anomalies based on NIDS. IEEE Latin America Transactions, 19(5), 772–779.
7) Dondapati, K. (2020). Integrating neural networks and heuristic methods in test case prioritization: A machine learning perspective. International Journal of Engineering & Science Research, 10(3), 49–61.
8) Panga, N. K. R. (2021). Financial fraud detection in healthcare using machine learning and deep learning techniques. International Journal of Management Research and Business Strategy, 10(3).
9) Sareddy, M. R. (2021). The future of HRM: Integrating machine learning algorithms for optimal workforce management. International Journal of Human Resource Management (IJHRM), 10(2), 5–16.
10) Mamidala, V. (2021). Enhanced security in cloud computing using secure multi-party computation (SMPC). International Journal of Computer Science and Engineering (IJCSE), 10(2), 59–72.
11) Basani, D. K. R. (2021). Leveraging robotic process automation and business analytics in digital transformation: Insights from machine learning and AI. International Journal of Engineering Research and Science & Technology, 17(3).
12) Prabhakaran, V., & Kulandasamy, A. (2021). Hybrid semantic deep learning architecture and optimal advanced encryption standard key management scheme for secure cloud storage and intrusion detection. Neural Computing and Applications, 33(21), 14459–14479.
13) Alturfi, S. M., Muhsen, D. K., Mohammed, M. A., Aziz, I. T., & Aljshamee, M. (2021). A combination techniques of intrusion prevention and detection for cloud computing. Journal of Physics Conference Series, 1804(1), 012121.
14) Ouiazzane, S., Addou, M., & Barramou, F. (2021). A Multiagent and Machine Learning based Hybrid NIDS for Known and Unknown Cyber-attacks. International Journal of Advanced Computer Science and Applications, 12(8).
15) Wang, W., Du, X., Shan, D., Qin, R., & Wang, N. (2020). Cloud Intrusion detection Method based on stacked Contractive Auto-Encoder and Support Vector Machine. IEEE Transactions on Cloud Computing, 10(3), 1634–1646.
16) Pise, N. (2021). Application of machine learning for intrusion detection system. Information Technology in Industry, 9(1), 314–323.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 18, Issue 1, 2022

17) Shyla, S. I., & Sujatha, S. (2020). An efficient automatic intrusion detection in cloud using optimized fuzzy inference system. International Journal of Information Security and Privacy, 14(4), 22–41.