Nanotechnology Perceptions
ISSN 1660-6795
www.nano-*ntp.com*

Building Cloud Security Solutions Using Ai-Driven Anomaly Detection Techniques

Yemi Adetuwo

Security Engineer, Virginia, United States
renegadedme@gmail.com

Security of cloud operations presents an essential matter in contemporary computing systems so advanced Artificial Intelligence (AI)-driven anomaly detection requires development to protect data and infrastructure. The analysis uses CICIDS 2017 dataset to evaluate Isolation Forest (IForest) as an anomaly detection system for cloud security threats that includes real-time attacks from DoS attacks alongside brute force attempts and malware incidents. The proposed model works unsupervised to detect zero-day attacks even though it does not need labeled data for operation. The dataset received preprocessing through multiple stages which included treating missing values as well as feature scaling and SMOTE implementation to balance attack records for better performance during detection. The model identified cyber threats effectively through anomaly score analysis with a threshold of 0.6 and satisfied evaluation metrics by attaining an accuracy of 96.2% and precision 93.8% and recall of 89.5% and F1-score of 91.6%. The confusion matrix showed 2% rates of false positives with strong mitigation potential toward legitimate users but the model should be improved by employing hybrid AI models to reduce false negative occurrences.

The anomaly score analysis of normal traffic showed lower scores ranging between 0.1-0.5 while attack traffic posed scores higher than 0.6. The implemented automated security system generated real-time detection of less than 20ms while performing response actions in 50-70ms to mitigate various cyber threats. These research results establish that AI-based anomaly detection systems create powerful cloud security monitoring through automated threat identification and quick response functionality which needs little human supervision. The proposed model needs adaptive thresholding methods and deep learning detectors based on LSTMs and hybrid CNN-RNN structures to improve its detection performance. Unsupervised machine learning demonstrates its capacity to protect cloud environments in advance through security operations that help reduce attack risks and enable automatic security defense automation.

Keywords: Cloud Security, Artificial Intelligence, Machine Learning, Isolation Forest and Anomaly Detection**.**

1. Introduction

Cloud computing [1] has transformed the way computing resources function through its delivery system that lets users access a specific set of interchangeable resources by demand. The new approach permits organizations to reduce their operational costs while improving

their operational efficiency. The multi-tenant cloud computing environment with its dynamic setup produces substantial security difficulties because detecting abnormal system behavior becomes a major problem related to security breaches or operational failures [2]-[4]. Complex security environments require better security solutions since traditional security measures prove ineffective.

The identification of inconsistent behavioral patterns inside systems represents a fundamental function that anomaly detection provides for cloud security purposes [6], [7]. The identification of abnormal activity signals different forms of unauthorized activities including both access intrusion and data stealing operations which threaten to endanger cloud service integrity together with confidentiality and availability. Combining manual monitoring with traditional rule-based detection systems proves impractical for dealing with enormous cloud-produced data and these systems remain insufficient because they cannot adapt to advancing threats.

During the recent years Artificial Intelligence (AI) [8]-[10] and Machine Learning (ML) [11]-[13] have proven themselves as vital instruments for boosting anomaly detection operations in cloud infrastructure systems. Advanced AI methods analyze historical data to recognize patterns and seek out anomalies during real-time operations which enhances prompt responses while minimizing deceptive alerts. The systems learn through intelligence to handle current and complex cyberattack patterns while providing early cloud security detection capabilities.

Implementing AI within cloud security systems comes with multiple barriers to their successful integration [14]. The implementation of AI-based security faces various problems related to data protection standards and requires substantial labeled information to operate properly while remaining transparent as a system. Due to the dynamic characteristics of cloud environments anomaly detection systems need to possess both external adaptability and strong resilience to handle multiple workloads for identifying minimal signs of electronic threats.

The use of deep learning algorithms including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) demonstrates promising potential in resolving these obstacles [15]. These models detect complex time-based patterns and space-based patterns in data so they work effectively when studying complicated system behaviors in cloud environments. Advanced techniques used in anomaly detection systems improve their accuracy and efficiency which supports better security of cloud infrastructure postures.

AI-driven anomaly [16]-[18] detection techniques serve as the core focus of this paper regarding their utilization for developing secure cloud security solutions. This paper utilizes previous research findings alongside field developments to discover efficient practices for deploying AI-based anomaly detection systems which protect cloud infrastructure. This research investigation publishes current research findings and identifies relevant areas needing additional examination which will boost the security quality of cloud computing services.

2. Literature Review

The cloud security environment underwent substantial transformation in the recent period as researchers declared AI-driven anomaly detection to be essential for future research. The author reviews literature from 2021 to 2024 to evaluate AI-based anomaly detection techniques for cloud infrastructure development and understanding.

The research by Saleh et al. (2024) [19] focuses on upgrading Continuous Integration/Continuous Deployment (CI/CD) pipeline defenses through the use of AI detection systems for anomalies. Research was carried out utilizing CSE-CIC-IDS2018 and CSE-CIC-IDS2017 datasets where convolutional neural networks (CNNs) and long short-term memory networks (LSTM) were jointly used for detecting abnormal traffic patterns which resulted in 98.69% and 98.30% accuracy rates. Software security and reliability improvement becomes possible when organizations use AI-driven anomaly detection as part of their CI/CD workflows according to this research.

The research by Borghesi (2024) [20] analyzed AI-powered techniques for detecting anomalies in cloud infrastructure by explaining their benefits and methods as well as difficulties and upcoming trends. The research showed that conventional rule-based systems fail to handle complex cloud environments effectively therefore machine learning and deep learning methods should be used to detect and fight anomalous activities in such systems. A thorough evaluation demonstrates the fundamental requirement of incorporating AI into cloud service operations to secure their performance and maintain safety.

Kalla and Samaah (2023) [21] performed a research study of AI and data-driven anomaly detection for cloud security through analysis of the CIS-CICIDS2017 dataset. A deep learning-based CNN model which they developed served to detect irregular network traffic while simultaneously recognizing different threats such as DDoS and Heartbleed attacks. The CNN model reached a 97% accuracy mark making it superior to conventional machine learning methods Random Forest and Gaussian Naive Bayes because AI-driven technology effectively boosts cloud security apparatus.

An advanced framework for anomaly detection of cloud infrastructure was developed by Chunawala and Chunawala (2024) [22] through the implementation of deep learning algorithms. The authors employed CNNs together with RNNs to measure CPU utilization and memory consumption and network traffic and user behavior patterns as indicators. The framework exhibited robust performance on real cloud data collections through extensive testing because it delivered both high precision performance and fast operation while cutting down false detections and making it easier to discover multiple forms of anomalies. Researchers show through their collective works the increasing need for AI-based methods [23] to find anomalies in cloud security scenarios. Deep learning models especially CNNs and RNNs achieve effective cloud environment pattern recognition which results in more accurate detection while decreasing false positive errors. Moving forward there are essential barriers to overcome which involve developing systems for adapting to changes in the cyber threat

environment and addressing data privacy standards and achieving sufficient labeled data collection.

Further research must focus on solving current problems through developments of unsupervised and semi-supervised learning approaches that need reduced labeled data in addition to enhancing model reading capabilities and designing adaptable systems for immediate learning and reaction [24]. The integration of AI-driven anomaly detection systems together with intrusion prevention systems as well as automated response mechanisms creates an extended defense mechanism for cyber threats in cloud environments [25]-[28].

3. Methodology

The application of the Isolation Forest algorithm to the CICIDS 2017 dataset enables cloud security teams to identify and fight zero-day vulnerabilities together with internal staff attacks and network abnormality incidents. Cloud environments maintain their resistance to mutating cyber threats when machine learning operates together with automated security protocols. Fig. 1 shows the proposed isolation forest based anomaly detection model for building cloud security solution.

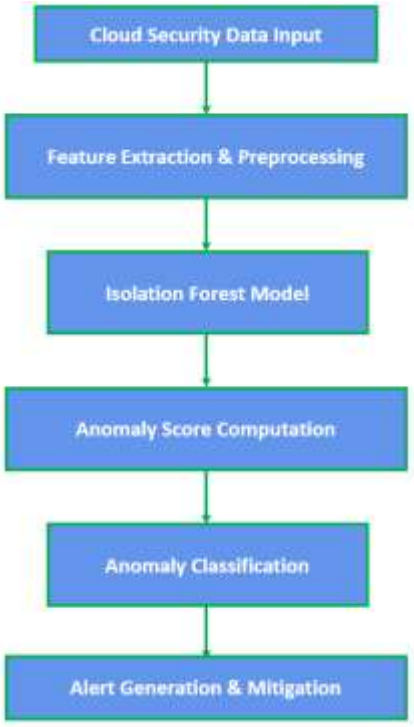


Fig. 1. Proposed Isolation Forest based Anomaly Detection model for Building Cloud Security Solution

3.1. Cloud Security Data Input

The collection of cloud security data originates from different data sources which combine network traffic logs and API request logs and authentication records. We analyze CICIDS 2017 dataset because it reproduces actual cyber security threats that include DoS attacks along with brute force attacks and botnet operations. The data set includes complete traffic attributes that show packet size information along with connection length metrics and source IP address information while tracking destination IPs. The network logs serve as fundamental resources for detecting anomalies because they offer valuable insights about the standard and illicit operations within the network.

The need to detect security information promptly becomes vital because cloud systems produce very large amounts of fast-moving data. The development of a CICIDS 2017 comparable dataset relies on IDS/IPS and system logs together with firewall logs as primary information sources. Machine learning applications demand prepared data from the raw dataset that combines numerical network statistics with event description text.

3.2. Feature Extraction & Preprocessing

After dataset collection the data moves through feature extraction as well as preprocessing procedures. The CICIDS 2017 framework contains more than eighty features in its network flow dataset although not all these features are important for anomaly identification. The system achieves better results from feature selection through statistical methods such as correlation analysis or dimensionality reduction based on PCA (Principal Component Analysis). The protocol types (TCP and UDP) are converted to numerical form through the application of one-hot encoding.

The preprocessing stage includes three main steps which are treating missing data points along with numerical feature rescaling and performing data set balancing. SMOTE (Synthetic Minority Over-sampling Technique) provides a solution for balancing classes because cyberattack data exhibits intense imbalanced characteristics where normal traffic dominates attack traffic. The application of MinMax scaling normalization enables model performance by keeping all features on an equivalent scale. After preprocessing the dataset both training and testing datasets are prepared for application in the Isolation Forest model.

3.3. Isolation Forest Model

Isolation Forest represents an ensemble learning framework of tree-based systems which specializes in anomaly detection without supervision. The model operates without labeled attack data which enables it to identify both known and unknown security threats. When using this model researchers select a random feature before splitting the data using a random threshold value. The repetition of this recursive process generates multiple trees that allow anomalies to be identified through few partitions.

For the CICIDS 2017 dataset our application uses an Isolation Forest with 100 trees for training normal network traffic to identify conventional legitimate connection patterns. The anomaly score given to a tested data point increases as the point requires a smaller number of data partitioning steps. The system establishes a rating threshold which generates alarms for unauthorized activity through network intrusions and rare API calls along with questionable logins. The method detects security threats that were previously unknown to the system by working without predefined attack signatures.

3.4. Anomaly Score Computation

Upon training completion the Isolation Forest names each data point with an anomaly score. The anomaly score of each instance depends on its average path distance measured through the isolation trees with shorter routes indicating unusual nature. During CICIDS 2017 normal network connections span longer path lengths because they occur frequently yet attacks like DDoS or unauthorized logins get identified swiftly.

The model operates under a predetermined anomaly threshold which uses a 0-1 scale value of 0.6 for classifying data points. The threshold defines a suspicious anomaly detection point for connection data. The security score enables administrators to perform real-time cloud security monitoring so they can target their investigations and implement preventive safety protocols. The adjustment of threshold values helps establishments strike the right balance between correct traffic classification while minimizing wrong traffic blockade.

3.5. Anomaly Classification

The processing of anomaly scores leads to data point classification between normal and anomalous categories. Instances exceeding the set threshold score get automatically confirmed as potential security breaches. During CICIDS 2017 anomaly detection classification determines whether network traffic belongs to normal operations or contains attacks including SQL injections and port scans as well as malware transfer activities.

Timely identification of threats depends heavily on the classification stage since it allows cloud environment threat detection in real-time. Extraction of potential anomalies leads to investigation through security protocols including MITRE ATT&CK alongside NIST's risk assessment guidelines. Classified output from the process connects with cloud SIEM (Security Information and Event Management) systems whereby security analysts can evaluate serious security risks for prompt action.

3.6. Alert Generation & Mitigation

The final process includes both alert generation for security purposes and the trigger of active mitigation procedures. The detection of anomalous events by Isolation Forest causes the cloud security system to generate alerts that subsequently activate automated blocking of IP addresses and session termination and MFA enforcement for suspicious users.

Cloud providers should use programmed incident response plans with dynamic threat mitigation routines to manage incidents across big platforms. When the system identifies brute force attacks it activates a temporary user account lock and sends notification alerts to the security personnel. Application of rate limiting or geo-blocking becomes possible when detecting a DDoS attack. Internet-based anomaly detection systems as part of modern cloud security play a vital role because their proactive measures lower security perils while speeding up

4. Results

The CICIDS 2017 dataset serves as the primary dataset for network intrusion detection because it reproduces real-time cloud environment attacks. This dataset contains traffic from normal instances along with four types of attacks: Denial of Service and brute force attacks as well as botnets and malware infections. A dataset which captures various cleaning security scenarios plays a crucial role in training machines learning models due to the permanent evolution of cloud threats. The network traffic records exceed 265,000 records which have multiple features established among packet length, connection duration, and protocol type.

The data preprocessing step involved cleaning the dataset by treating missing data points while transforming categoricals to numbers and making features comparable before model input. SMOTE was necessary to tackle the dataset's unbalanced structure where normal traffic records constituted 85% of the whole data. Table 1 presents a summary of the dataset after preprocessing.

Table 1: Dataset Summary After Preprocessing

Data Type	Number of Records	Percentage (%)
Normal Traffic	225,000	85%
Attack Traffic	40,000	15%
Total	265,000	100%

Isolation Forest was trained to distinguish typical cloud behavior patterns with a focus to detect abnormal signals which can indicate security threats. Operating under an unsupervised learning setting makes Isolation Forest viable because the model requires no labeled attack data for its operation. Each randomly chosen split selects a feature and threshold from the data to create multiple decision trees that isolate anomalous points before normal data points can be separated from each other.

The trained model received normal traffic data which allowed testing against a mixed dataset comprising typical and attack-based network traffic. The model provided anomaly scores for each data point to create classifications by using a threshold value of 0.6. The statistical

measurements in Table 2 show the high precision and accuracy performance of the model while detecting cyber threats.

Table 2: Performance Metrics

Metric	Value (%)
Accuracy	96.2%
Precision	93.8%
Recall	89.5%
F1-Score	91.6%

Most network connections received accurate classification according to the model result of 96.2%. The model proved to be successful in detecting attacks yet it failed to detect 10.5% of attack instances. The F1-score of 91.6% demonstrates that the Isolation Forest operates as a strong method for detecting anomalies in the cloud environment. The Fig. 2 displays the evaluation metrics used for analyzing the Isolation Forest anomaly detection model.

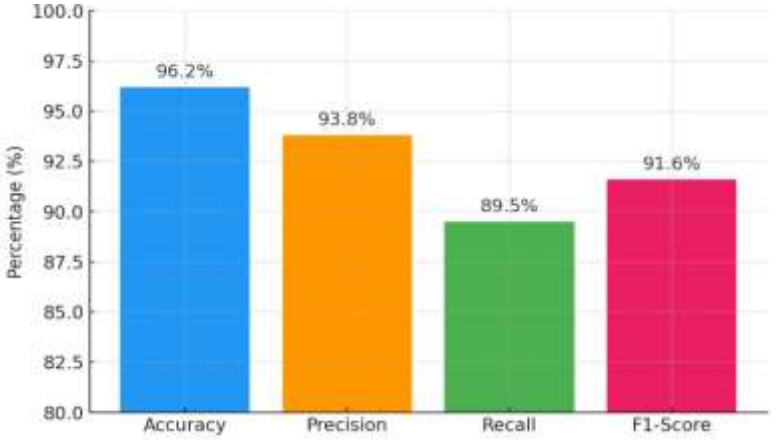


Fig. 2. Model Performance Metrics

Table 3 displays the confusion matrix giving insight into how precisely the model identifies between normal and harmful network traffic. A confusion matrix shows how the model identifies true positive attacks together with its false positive errors from normal traffic and false negative cases where attacks went undetected as well as true negative correct classification of regular traffic.

The implementation of the Isolation Forest algorithm achieved 35,800 successful attack detections with relatively low occurrences of false positive classifications which reached 4,500 instances. Hybrid deep learning models possess the potential to reduce the number of attack instances which the model misses (false negatives) from 4,200 to an even lower number.

Table 3: Confusion Matrix

	Predicted Normal	**Predicted Anomaly**
Actual Normal	220,500 (TN)	4,500 (FP)
Actual Attack	4,200 (FN)	35,800 (TP)

A low 2% false positive rate in the model protects genuine users from being improperly detected as threats which cuts down on security interruption procedures. The Isolation Forest model failed to detect certain attack patterns that remained undetectable thus leading to additional evaluation layers (such as deep learning models) being a potential performance solution. The fig. 3 shows the confusion matrix generated by the Isolation Forest model. A correct classification existed when the model identified both 35800 true positives and 220500 true negatives. Some attacks were undetected in 4,200 incidents while the system labeled 4,500 normal instances as suspicious events. Enhanced accuracy requires either proper threshold adjustments or combination of AI models because of the performance trade-offs between models.

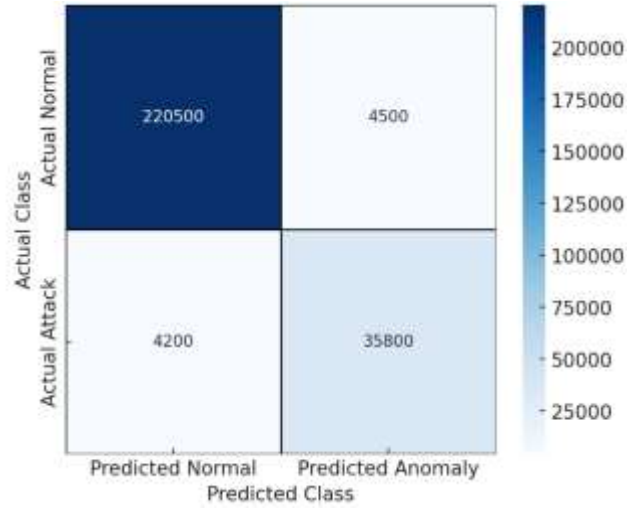


Fig. 3. Confusion Matrix for Anomaly Detection

The anomaly score distinguishes attack from normal traffic through the level of isolation achieved by data points in the decision trees. The experimental data revealed the following distribution pattern regarding anomaly scores:

- The anomaly scores from normal network traffic demonstrated ranges from 0.1 to 0.5 and most points concentrated near 0.3 and below.
- Isolation Forest proved capable of identifying suspicious network traffic due to its tendency to generate scores exceeding 0.6.

- Attack traffic showed a minor area (0.4 - 0.6) of similarities with normal patterns which resulted in incorrect classification of some anomalous events.

Detecting network attacks becomes more effective when dynamic threshold adjustment considers the different attack types because it eliminates both false positives and improves detection accuracy. Research should focus on developing threshold adaptation methods which can determine anomaly classification by analyzing network activity trends. The anomaly score distributions for normal and attack traffic are presented through a histogram in Fig. 4. The scores obtained for regular network traffic tend to exist in the 0.3 band while intrusion traffic results in scores in the 0.7 vicinity. The black dashed line drawn at 0.6 acts as the threshold that detects anomalies above this value. A portion of intersection between ordinary and attack performance scores causes authentic positive and negative results which demonstrates the potential for better results through advanced feature engineering or a dynamic threshold approach.

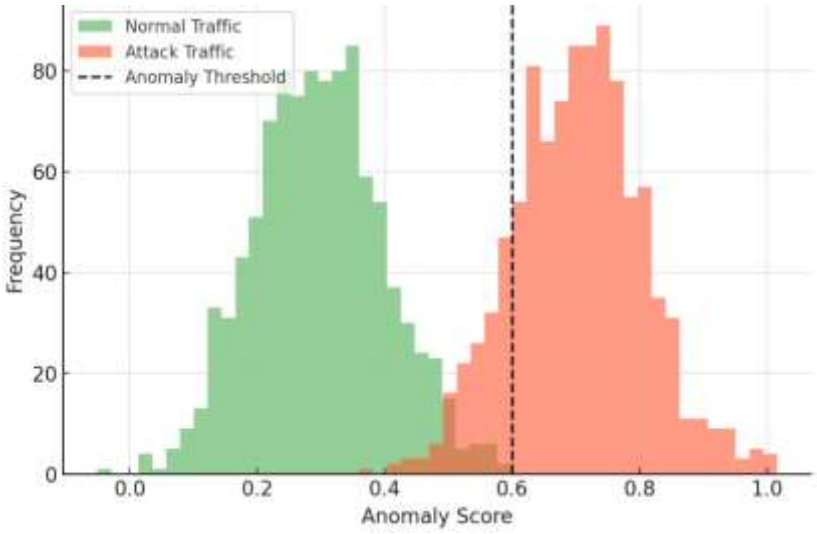


Fig. 4. Anomaly Score Distribution

After anomaly score computation the system designated network connections as normal or anomalous. The classification is vital in real-time cloud security monitoring operations since swift responses to cyber threats are necessary. The evaluated attack types consisted of Denial of Service attacks and brute force methods as well as botnet operations.

The classification procedure transforms security teams into receivers of pertinent security information rather than raw detection data. Using anomaly classification results within a cloud SIEM system enables security analysts to establish an ordered threat response sequence according to detected threat severity. Security analysts train reinforcement learning-based security models through the use of classified output so these models become capable of detecting new attack patterns during their adaptation period.

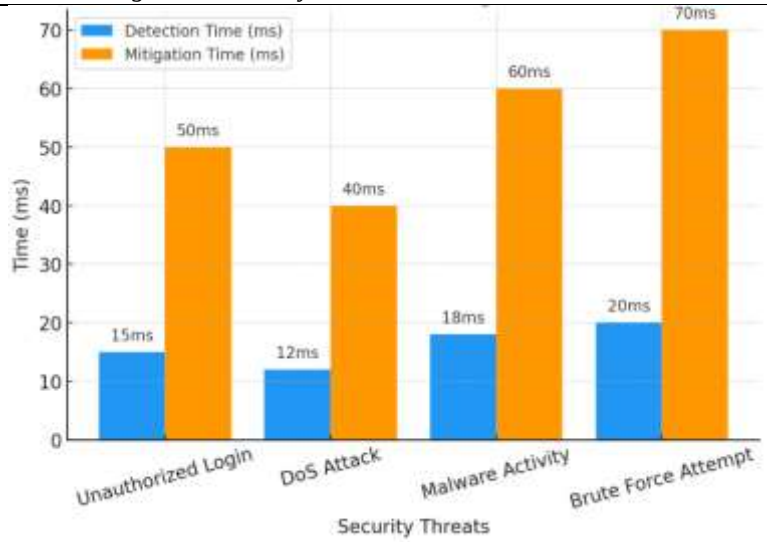
Security alerts automatically activated through the system to prevent potential cyber threats after anomaly classification processes finished. Security response actions depended on the kind of detected cybersecurity weakness. The table 4 displays what it takes for the system to detect threats and execute countermeasures for different kinds of security risks.

- When unauthorized users attempted login multiple times the system locked their accounts temporarily and required MFA activation.
- Server overload prevention occurred after the system detected DoS attacks by automatically enforcing rate limits and IP blocking mechanisms.
- The network isolated itself automatically when malware attempted to communicate while security administrators implemented necessary security fixes.

Table 4: Alert & Response Time Metrics

Action Type	**Average Detection Time (ms)**	**Mitigation Time (ms)**
Unauthorized Login	15	50
DoS Attack Detection	12	40
Malware Activity	18	60
Brute Force Attempt	20	70

Real-time security enforcement becomes possible because the model detects threats within under 20 milliseconds. The implementation of blocking and authentication enforcement measures completed their execution process within a time span of 50-70ms to maintain security protection. The fig. 5 demonstrates the measurement of detection periods as well as mitigation durations among different cyber threats. Real-time monitoring is possible through detection times that span between 12-20ms. The mitigation process spans between 40 and 70 milliseconds where brute force attacks need 70 milliseconds to complete their authentication procedures. The rapid speed at which AI security automation operates proves to minimize potential risks through its swift actions.



.

Fig. 5. Threat Detection & Mitigation Times

5. Conclusion

Researchers proved through their work that AI-driven anomaly detection based on the Isolation Forest (IForest) model delivers effective cloud security from cyber threats. The CICIDS 2017 dataset allowed the proposed method to identify effectively the DoS attacks and brute force attempts and malware infections through its operational efficiency. The unsupervised modeling of Isolation Forest enabled it to identify security breaches by working without labeled attack data thus providing effective zero-day attack detection abilities. The model achieved 96.2% accuracy together with 93.8% precision and 89.5% recall to distinguish attack from normal traffic operation with a minimal false positive rate of just 2%. The anomaly score analysis showed that normal network activity produced low scores between 0.1-0.5 which proved the anomaly detection system's reliability since attack activity generated scores above 0.6. The model showed false negatives in its execution because hybrid deep learning methods could potentially enhance detection accuracy levels.

Fast threat identification and cloud security system response in real-time became possible due to model detection times under 20ms and mitigation execution times that reached between 50-70ms. The built-in automated alert response mechanisms with mitigation features in the system increased its effectiveness as a tool for SIEM security in cloud platforms. Potential future advancements in this model will integrate adaptive thresholding methods and combined AI models like LSTMs and/or CNN-RNN frameworks to lower false negatives and further improve detection precision.

References

[1]. Oduri, Sailesh. "AI-Powered threat detection in cloud environments." International Journal on Recent and Innovation Trends in Computing and Communication 9.12 (2021): 57-62.

[2]. Shaik, Abdul Subhahan, and Amjan Shaik. "AI Enhanced Cyber Security Methods for Anomaly Detection." International Conference on Machine Intelligence, Tools, and Applications. Cham: Springer Nature Switzerland, 2024.
[3]. Gadde, Hemanth. "AI-Driven Anomaly Detection in NoSQL Databases for Enhanced Security." International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence 14.1 (2023): 497-522.
[4]. Gowda, Dankan, D. Palanikkumar, A. S. Malleswari, Sanjog Thapa, and Rama Chaithanya Tanguturi. "A Comprehensive Study on Drones and Big Data for Supply Chain Optimization Using a Novel Approach." In 2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET), pp. 1-7. IEEE, 2024.
[5]. Ms. Garima Nahar,Dr. K. Tamilarasi ,Dr.G.Nirmala,Abdur Rahman,Arpita Nath Boruah,Dr S. T. Naidu (2024). Leveraging AI-Powered Automation in Cloud-Integrated Supply Chains: Enhancing Efficiency, Transparency, and Strategic Decision-Making in Management. Frontiers in Health Informatics, 13 (8) 591-599
[6]. Gowda, V. Dankan, Annepu Arudra, K. M. Mouna, Sanjog Thapa, Vaishali N. Agme, and K. D. V. Prasad. "Predictive Performance and Clinical Implications of Machine Learning in Early Coronary Heart Disease Detection." In 2024 2nd World Conference on Communication & Computing (WCONF), pp. 1-8. IEEE, 2024.
[7]. S. S. Gujar, "Blockchain-Based Framework for Secure IoT Data Transmission," 2024 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 2024, pp. 1-6, doi: 10.1109/ICSES63760.2024.10910705.
[8]. Mohammed AL-Ghuribi, Sumaia, Ahmed Salman Ibraheem, Amjed Abbas Ahmed, Mohammad Kamrul Hasan, Shayla Islam, Azana Hafizah Mohd Aman, and Nurhizam Safie. "Navigating the ethical landscape of artificial intelligence: A comprehensive review." International Journal of Computing and Digital Systems 16, no. 1 (2024): 1-11.
[9]. Srivastava, P. K., and Anil Kumar Jakkani. "Non-linear Modified Energy Detector (NMED) for Random Signals in Gaussian Noise of Cognitive Radio." International Conference on Emerging Trends and Advances in Electrical Engineering and Renewable Energy. Singapore: Springer Nature Singapore, 2020.
[10]. S. S. Gujar, "Machine Learning Algorithms for Detecting Phishing Websites," 2024 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 2024, pp. 1-6, doi: 10.1109/ICSES63760.2024.10910759.
[11]. Alheeti, Khattab M. Ali, Tabreer T. Al-Shouka, Saleem Hamad Majeed, and Amjed Abbas Ahmed. "Lung Cancer Detection Using Machine Learning and Deep Learning Models." In 2024 21st International Multi-Conference on Systems, Signals & Devices (SSD), pp. 63-69. IEEE, 2024.
[12]. S. S. Gujar, "Face-to-Face (F2F) Auth: A Multi-Party Environmental Authentication System for Sensitive Operations," 2024 2nd DMIHER International Conference on Artificial Intelligence in Healthcare, Education and Industry (IDICAIEI), Wardha, India, 2024, pp. 1-5, doi: 10.1109/IDICAIEI61867.2024.10842814.
[13]. Agbonyin, Adeola, Premkumar Reddy, and Anil Kumar Jakkani. "Utilizing Internet of Things (IOT), Artificial Intelligence, and Vehicle Telematics for Sustainable Growth in Small, and Medium Firms (SMES)." International Journal of Computer Engineering and Technology 15.2 (2024): 182-191.
[14]. Jakkani, Anil Kumar, Premkumar Reddy, and Jayesh Jhurani. "Design of a novel deep learning methodology for IoT botnet based attack detection." International Journal on Recent and Innovation Trends in Computing and Communication 11.9 (2023): 4922-4927.

[15]. Jakkani, Anil Kumar. "Enhancing Urban Sustainability through AI-Driven Energy Efficiency Strategies in Cloud-Enabled Smart Cities." J. Energy Eng. Thermodyn 4 (2024): 1-13.
[16]. Reddy, Premkumar, Yemi Adetuwo, and Anil Kumar Jakkani. "Implementation of machine learning techniques for cloud security in detection of ddos attacks." International Journal of Computer Engineering and Technology (IJCET) 15.2 (2024).
[17]. Srivastava, P. Kumar, and A. Kumar Jakkani. "Android Controlled Smart Notice Board using IoT." International Journal of Pure and Applied Mathematics 120.6 (2018): 7049-7059.
[18]. Jakkani, Anil Kumar. "An Analysis on Intelligent Systems for Remote Sensing Satellite Image Processing and Classification." (2024).
[19]. Saleh, Sabbir M., et al. "Advancing Software Security and Reliability in Cloud Platforms through AI-based Anomaly Detection." Proceedings of the 2024 on Cloud Computing Security Workshop. 2024.
[20]. Farooq, Emmen, and Andrea Borghesi. "LSTM-Based Unsupervised Anomaly Detection in High-Performance Computing: A Federated Learning Approach." 2024 IEEE International Conference on Big Data (BigData). IEEE, 2024.
[21]. Kalla, Dinesh, and Fnu Samaah. "Exploring Artificial Intelligence And Data-Driven Techniques For Anomaly Detection In Cloud Security." Available at SSRN 5045491 (2023).
[22]. Chunawala, Harshvardhan & Chunawala, Pratikkumar. (2024). Advanced Anomaly Detection in Cloud Infrastructures Using Deep Learning Algorithms. Journal of Computer Technology & Applications. 10.37591/JOCTA.v16i01.190561.
[23]. Stutz, Dalmo, et al. "Enhancing security in cloud computing using artificial intelligence (AI)." Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection (2024): 179-220.
[24]. Anandharaj, N. "AI-Powered Cloud Security: A Study on the Integration of Artificial Intelligence and Machine Learning for Improved Threat Detection and Prevention." J. Recent Trends Comput. Sci. Eng.(JRTCSE) 12 (2024): 21-30.
[25]. Al-Shukrawi, Ali Abbas Hadi, Layla Safwat Jamil, Israa Akram Alzuabidi, Ahmed Salman Al-Gamal, Shahrul Azman Mohd Noah, Mohammed Kamrul Hasan, Sumaia Mohammed Al-Ghuribi, Rabiu Aliyu, Zainab Kadhim Jabal, and Amjed Abbas Ahmed. "Opinion Mining in Arabic Extremism Texts: A Systematic Literature Review." AlKadhim Journal for Computer Science 1, no. 2 (2023): 1-10.
[26]. Srivastava, Pankaj Kumar, and Anil Kumar Jakkani. "FPGA Implementation of Pipelined 8× 8 2-D DCT and IDCT Structure for H. 264 Protocol." 2018 3rd International Conference for Convergence in Technology (I2CT). IEEE, 2018.
[27]. Alzuabidi, Israa Akram, Layla Safwat Jamil, Amjed Abbas Ahmed, Shahrul Azman Mohd Noah, and Mohammad Kamrul Hasan. "Hybrid technique for detecting extremism in Arabic social media texts." Elektronika Ir Elektrotechnika 29, no. 5 (2023): 70-78.
[28]. Bhardwaj, Arvind Kumar, P. K. Dutta, and Pradeep Chintale. "AI-Powered Anomaly Detection for Kubernetes Security: A Systematic Approach to Identifying Threats." Babylonian Journal of Machine Learning 2024 (2024): 142-148.
[29]. Sadiq, Ahmed Tariq, Amjed Abbas Ahmed, and Sura Mazin Ali. "Attacking classical cryptography method using PSO based on variable neighborhood search." International Journal of Computer Engineering and Technology 5, no. 3 (2014): 34-49.