Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS-2025)
IEEE Xplore Part Number: CFP25K74-ART; ISBN: 979-8-3315-1208-8

2025 International Conference on Intelligent Computing and Control Systems (ICICCS) | 979-8-3315-1208-8/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICICCS65191.2025.10984898

# Threat Eye: Behavior Analytics for Cloud Security using ML

[1]J. R. V. Jeny, [2]S. Shivaspandana, [3] K. Pavan, [4]N. Muthukumaran, [5]K. Akash
[1, 4]Professor, [2,3,5]UG scholar
[1,2,3,5] Department of Computer Science and Engineering (AI & ML)
Vignan Institute of Technology and Science-508284
[4] Professor, Centre for Computational Imaging and Machine Vision, Department of ECE, Sri Eshwar College of Engineering, Coimbatore, India.
E-mail: jeny.navagar18@gmail.com, shivaspandanasreevari@gmail.com, goudpavan77@gmail.com, kumaranece@gmail.com, koudaaksh21@gmail.com

**ABSTRACT:** Cloud computing has developed for its storage and accessibility of data, providing flexibility, scalability, and affordability. But its extensive use has also resulted in cyberattacks and unauthorized access. The traditional intrusion detection mechanisms become ineffective for different attack patterns, insider attacks and zero-day exploits. This paper provides an efficient way to address this issue by providing a mechanism to identify the threat based on the behaviour of the user. Unlike traditional approaches this paper provides a system that monitors the user behaviour patterns considering the features such as login history, authentication attempts, session duration, file access activities, password change frequency and IP location modifications. By considering these features the attack can be detected, and the data access is restricted to prevent from unauthorized access. This paper provides handling of attack with a combination of machine learning algorithms including SVM, Decision tree and XBoost, these help in distinguishing between the attacker and the authorized user. This helps in identifying complex attack behaviours and detect insider threats. Additionally, RSA encryption is integrated to secure data transmissions, preventing unauthorized access. By combining behavioural analysis, attacks prediction, and encryption, this provides a robust cybersecurity framework.

**Keywords:** *Cloud Security, Machine Learning (ML), Cyber Threat Detection, Data Protection, Data Security, Gradient Boosting Classifier, Logistic Regression, Voting Classifier.*

## I. INTRODUCTION

In Progress, the technologies have been evolving, requirement for efficient attacks detection is also necessary. The traditional network-based intrusion detection is not sufficient anymore. The present intrusion detection systems mainly use signature-based approaches. It is effective in identifying traditional threats, the systems fail to detect zero-day attacks, insider attacks, and behavioral anomalies, leading to high false positive and false negative rates. They also lack adaptive learning, which reduces their effectiveness in detecting new and emerging threats within cloud environments. To handle these limitations, the paper provides an effective method of providing a threat eye that continuously monitors the user behaviour. This considers the features such as login counts, unsuccessful login attempts, session durations, file access history, location-based access alterations. From this that the system can recognize suspicious behaviours that can identify an attack, for example, illegal file access or repeated failed logins. The advantage of this approach is its adaptive learning that helps as self-learning ability. Whenever an attack is detected, the system immediately restricts access, so that it prevents data breaches. If no threat is detected, a secure decryption key is transmitted to

the intended recipient, ensuring only authorized users can access sensitive data. As this uses the combination of ML algorithms it provides an efficient way of preventing unauthorized access. This approach not only ensures the cloud security but also removes insider threats and zero-day attacks by utilizing behaviour analytics.

## II. RELATED WORK

Uses a hybrid feature selection approach with ML classifiers to improve cloud IDS efficiency. Focuses only on detection, lacks encryption for data protection [1]. Introduces autonomous federated learning for distributed IDS in public networks. Lacks security measures for stored/transmitted data in case of attack. The proposed approach ensures sensitive files remain inaccessible even if an intrusion occurs [2].

This paper integrates a modified Firefly Algorithm with ML models for cloud intrusion detection. IDS efficiency is improved, but data confidentiality is not addressed [3]. Uses LSTM and FNN to enhance IDS for SCADA power grids. Focuses on detecting cyber threats in critical infrastructure system. Designed for power grid security, making it less adaptable to general cloud environments [4]. In this paper it Proposed GenCoder, an adaptive AI-based IDS for vehicle cybersecurity. Uses generative AI to enhance real-time attack detection within intra-vehicle networks. Focuses on intrusion detection, does not prevent unauthorized data access [5].

Detects real-time intrusions using deep learning for IoT cybersecurity but lacks post-attack data security and only detects threats [6].

This paper provides ML and deep learning techniques for anomaly detection in cloud networks. Theoretical study with no implementation of encryption-based security [7].

Protects cloud networks from brute-force and DDoS attacks using an IDS framework. Focuses only on external threats but does not protect internal sensitive data. [8]. Introduces SEPCVN, a secure protocol for cloud vehicular networking. Enhances data communication security in cloud-based vehicle systems. Focuses on secure communication but does not address stored data encryption [9]. Uses blockchain-based federated learning for intrusion detection. Uses bidirectional long short-term memory (BiLSTM) for improved threat detection. High computational cost makes real-time processing challenging [10]. Detects privilege escalation attacks in cloud environments using ML-based analysis. Uses ensemble ML algorithms such as XGBoost and LightGBM. Detects attacks but does not prevent unauthorized data access [11].

Proposes an overhead reduction technique for SDN-based IDS to improve efficiency. Uses a Naïve Bayes Protection System to reduce system resource usage. Reduces IDS processing overhead but lacks measures to secure stored data [12]. Uses ensemble learning to enhance IDS performance by stacking multiple AI models. Uses multiple AI models, including bagging and stacking, for classification. Focuses on detection but does not implement post-attack data protection [13]. Enhances security of host-based IDS in IoT using ML-based fuzzy systems. Combines Decision Tree, Gradient Boost, and Random Forest models. High false positive rates lead to inefficiency in real-world applications [14]. Uses ML to detect and categorize anomalies in multi-cloud environments. Uses unsupervised learning techniques to detect unusual cloud activities. Detects anomalies but lacks post-detection security mechanisms [15].

## III. METHODOLOGY

In the growing technologies, security has raised major importance in every individual. The attacks that are of different patterns are evolving. The traditional signature-based detects known network attacks like Denial-of-Service (DoS), Probe, User-to-Root (U2R), and Remote-to-Local (R2L) attacks. These systems are ineffective with zero-day attacks, insider threats, and behavioral anomalies, resulting in high false positive and false negative rates. The proposed system will ensure that it is not limited to network based attacks. It also considers the behavioral variations of the user. It involves

adaptive learning so that to help in detecting cyber threats. With this it also helps in detecting the insider threats. Let us consider the flow of the paper in Figure 1 below.

Initially the owner uploads a file in the cloud with the specific recipient. Now here the authorization of the user is essential. So, the behavior of the user is considered instead of directly giving access. To determine whether the user is correct one or not this proposed system considers some features of the user that decides whether to give access to the user or not. Table 1 shows the features that are considered for detecting the authorization of the user. By considering these parameters the unusual behavior of the user is known. This helps in identifying the threat and resolving the security concerns.

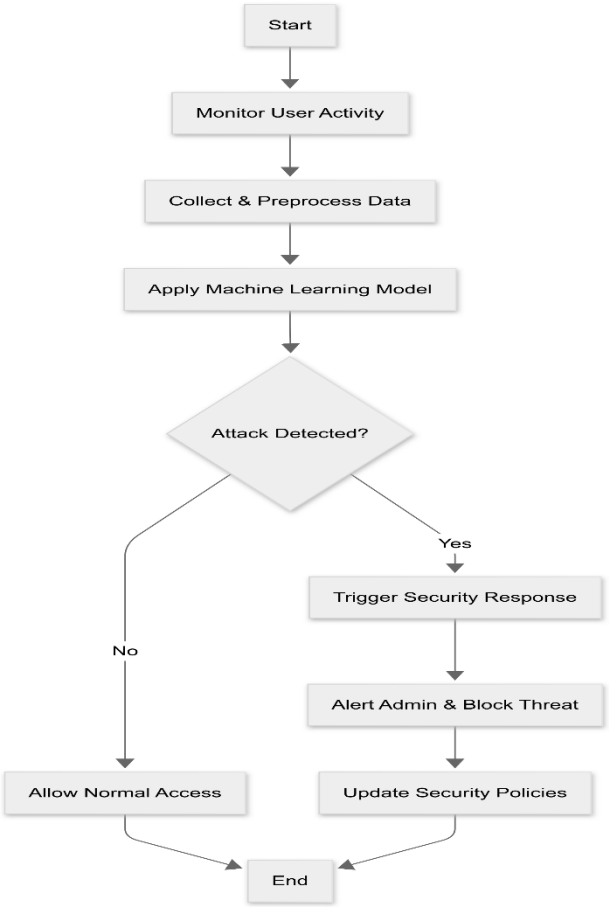


**Figure 1: Working Model Flowchart**

| Feature | Description | Usage |
|---|---|---|
| Login Frequency | Number of times a user logs in within a specific period | Unusual login frequency may indicate unauthorized access attempts. |
| Failed Login Attempts | Number of incorrect logins attempts before a successful login. | A high number suggests brute-force attacks or credential stuffing. |
| Data Transferred (MB) | Total amount of data uploaded/downloaded by the user. | Unusual data transfer could indicate data exfiltration or theft. |
| Session Duration | Total time the user is active in a session. | Long or short session durations outside normal behavior could signal anomalies. |
| Accessed Files | Number of files accessed by the user in a session. | Accessing an unusually high number of files may indicate an insider threat. |
| Password Changes | Number of times the user changes their password. | Frequent password changes could indicate an attacker trying to gain control. |
| IP Location Changes | Number of times the user logs in from different geographic locations. | Frequent or suspicious IP changes suggest account compromise. |
| Suspicious URL Clicks | Number of times the user clicks on links flagged as suspicious. | Clicking on phishing links may indicate social engineering attempts. |
| Time Since Last Login (Hours) | The gap between the previous and current login. | Large gaps followed by unusual behaviour could indicate account compromise. |

**Table 1: Behavioural Parameters for Cloud Security Threat Analysis**

So, after collecting this information of the user then this data is pre-processed and used in further. Now in this we use combination of ML models to get effective detection and handling of the attack. Each algorithm plays it role in detecting or classifying the type of the attack. The Random Forest classifier will build multiple decision trees and combines their output. In this approach RF is used in classifying user sessions as normal or suspicious based on the Table 1. The SVM is used as it helps classify user sessions as normal or suspicious based on features like login frequency, session duration, and failed login attempts. It forms a decision boundary which separates normal users and attackers. It Handles

high-dimensional and complicated data well. Now the Logistic Regression provides probability-based classification for handling attacks. It evaluates attack based on the patterns of the behaviour. For example, if a user frequently changes his/her passwords and opens files from unusual locations, then the model will classify the activity as suspicious with a high probability.

Gradient Boosting Classifier is effective in identifying attacks such as insider threats, unauthorized file access, and abnormal login behaviours. Its ability to detect this type of attacks makes it a valuable tool for cloud security. It is highly accurate and efficient in handling complex attack behaviours. It can learn from previous misclassifications to improve detection. It also reduces false positives by targeting difficult-to-classify cases. Now the performance of these algorithms is combined and evaluated with the voting classifier. It works with two models that is hard and soft voting. It Reduces dependency on a single model, improving overall performance. Here Hard voting ensures stability, while soft voting provides probabilistic flexibility. By combining SVC, Logistic Regression, and Gradient Boosting, the Voting Classifier strengthens intrusion detection based on the behavioural principles. These algorithms work together by initially collecting user activity data including login attempts, session duration, and file access patterns. Key behavioural features are identified from the data for training the ML models. Each classifier is trained on historical data. Their performance is now compared based on accuracy and precision. After considering the output from all the different classifiers the conclusion is made. If an attack is detected, then it will trigger the security response. It also alerts the admin and blocks the user accessibility. So that the data is kept secure from unauthorized access. If no attack is detected, then that says there is no harm. In this case the decryption key is securely given to the user for accessing the files. So here the data is secured from unauthorized access and the behaviour-based attacks are detected and handled.

## IV. RESULT AND DISCUSSION

Behavior-based attacks are detected and thus security is provided. This uses a combination of multiple algorithms by comparing their outcomes od accuracy.

**Table 2: Accuracy Comparison of Different Algorithms**

| Algorithm | Accuracy (Percentage) |
|---|---|
| SVM | 42.71% |
| Logistic Regression | 38.84% |
| Gradient Boosting Classifier | 97.09% |
| Voting Classifier | 67.98% |

The above Table 2 shows the list of algorithms and their accuracy in detecting an attack based on the user behavior. We can see that the SVM and logistic regression are not giving high accuracy. They are given up to 42.71% and 38.84%. Whereas the gradient boosting classifier had produced accuracy up to 97.09%. The voting classifier also provides reasonable accuracy while it is also helpful in combining all the models.

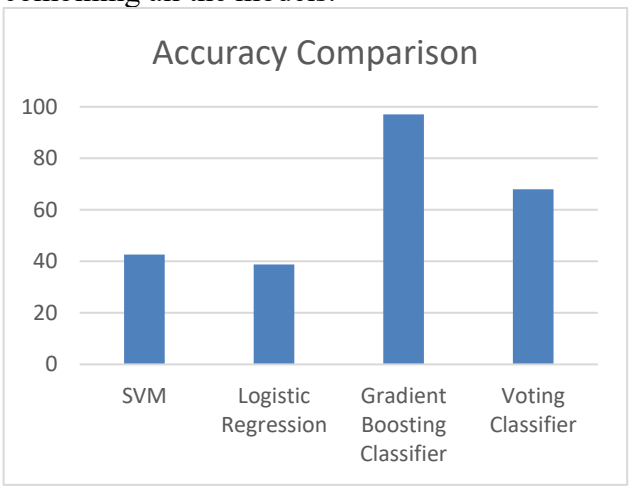


**Figure 2: The Accuracy of Machine Learning Algorithms Used.**

Figure 2 shows the visual representation in the form of a bar graph that depicts the accuracy of the algorithms. The outcomes of this proposed approach can be seen in Figure 3.

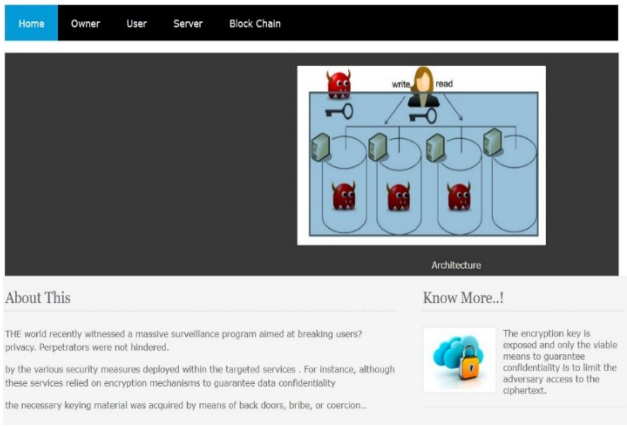


**Figure 3: Home Page of the Threat Eye**

In Figure 3, the home page shows that it includes about the system and navigation. The registration page of the owner can be seen as in Figure 4.

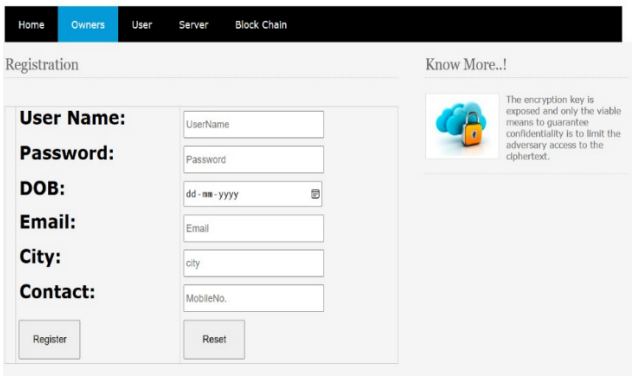


**Figure 4: Registration Page of the Owner**

After the owner uploads the file and user who wants to access the file, behavior of his is observed by the parameters in Table 1 and if there is any threat or suspicious activity detected then the alert is generated. This then stops the user from accessing the data. Thus, the information in the cloud is protected. On the high utilization of cloud services, it is very important to enable security measures. The Threat eye is an approach to behavior analytics for providing cloud security that is by using a hybrid model i.e. combination of models. Here the SVM, logistic regression has given lower accuracy in detecting various patterns, but the gradient boost is providing good outcome. In further it can also be improved with real time monitoring so that the attacks are handled efficiently. Hence this approach of detecting attack or threat that is by behaviour of the user that is more importantly used in detecting insider threats is given. The increasing complexity of cyber threats in cloud environments now a days requires solutions for detecting the attack and ensuring resolving measures. This approach is overcoming that difficulties in providing to detect the attack.

## V. CONCLUSION AND FUTURE SCOPE

In conclusion, the paper provides a behavior-based attack detection system that is implemented in a cloud environment using multiple machine learning models. Unlike traditional approaches as static rules or signature-based intrusion detection, where known network attacks are the focus, this system detects threats by monitoring user behaviour. Instead of allowing attackers to exploit the data this approach will block and provides alert to the admin. The behaviour dataset is pre-processed, divided, and trained using SVC, Logistic Regression, Gradient Boosting Classifier, and Voting Classifier, with accuracy comparison to determine which the best performing model is. The selected model is implemented in the cloud to track user behaviour like failed logins, data transfer, IP location change, and suspicious URL clicks. On detection of an attack then the access is blocked, and the data is available to the authorized user only. Ensemble learning techniques enhance the accuracy of detection and reduce false positives. The system effectively identifies known and unknown attack patterns, improving cloud security. By using machine learning-based behavior analysis, this approach demonstrates a more robust and responsive approach to cyber threat detection.

As cyber threats continue to evolve, there is significant importance for improving intrusion detection system. In future this can be modified by integrating with Deep Learning Models that can include the application of neural networks like LSTMs or Autoencoders to enhance anomaly detection precision. Real-time Monitoring can be applied to the system to detect threats in real-time using streaming data analytics. Adding blockchain-

based authentication can also improve cloud data security. Integrating blockchain technology to store and verify user activity logs could prevent data tampering. Cloud-based deployment with scalable architecture using technologies such as Kubernetes and serverless computing would improve scalability, enabling real-time monitoring of extensive cloud networks. Adding AI-based automated response systems may enable the system to hold, investigate, and neutralize threats independently without direct human intervention.

## REFERENCES

[1]. Bakro, M., Kumar, R. R., Alabrah, A., Ashraf, Z., Ahmed, M. N., Shameem, M., & Abdelsalam, A. (2023). An improved design for a cloud intrusion detection system using hybrid features selection approach with ML classifier. *IEEE Access*, *11*, 64228-64247.

[2]. Mahmoodi, A. B. Z., Sheikhi, S., Peltonen, E., & Kostakos, P. (2023). Autonomous federated learning for distributed intrusion detection systems in public networks. *IEEE Access*, *11*, 121325-121339.

[3]. Rana, P., Batra, I., Malik, A., Ra, I. H., Lee, O. S., & Hosen, A. S. (2024). Efficacious Novel Intrusion Detection System for Cloud Computing Environment. *IEEE Access*

[4]. Rajassekharan, Dinesh, and Abbylashnny A. Murugan. "An Efficient Analysis of Cloud-based Energy Management System for Secure Data Transmission." Journal of Electrical Engineering and Automation 6, no. 4 (2024): 289-299.

[5]. Kandhro, I. A., Alanazi, S. M., Ali, F., Kehar, A., Fatima, K., Uddin, M., & Karuppayah, S. (2023). Detection of real-time malicious intrusions and attacks in IoT empowered cybersecurity infrastructures. *IEEE Access*, *11*, 9136-9148.

[6]. Abdallah, A., Alkaabi, A., Alameri, G., Rafique, S. H., Musa, N. S., & Murugan, T. (2024). Cloud network anomaly detection using machine and deep learning techniques-recent research advancements. *IEEE Access*.

[7]. Nadeem, M., Arshad, A., Riaz, S., Band, S. S., & Mosavi, A. (2021). Intercept the cloud network from brute force and DDoS attacks via intrusion detection and prevention system. *IEEE Access*, *9*, 152300-152309.

[8]. P. M. Naidu; N. Muthukumaran; S. Chandralekha; K. Tejaswini Reddy; K.Sri Vaishnavi, "An Analysis on Virtual Mouse Control using Human Eye," 2024 5th International Conference on Image Processing and Capsule Networks (ICIPCN), Dhulikhel, Nepal, 2024, pp. 233-237, doi: 10.1109/ICIPCN63822.2024.00045.

[9]. Mbaya, E. B., Adetiba, E., Badejo, J. A., Wejin, J. S., Oshin, O., Isife, O., ... & Adebiyi, E. F. (2023). SecFedIDM-V1: A secure federated intrusion detection model with blockchain and deep bidirectional long short-term memory network. *IEEE Access*, *11*, 116011-116025.

[10]. Mehmood, M., Amin, R., Muslam, M. M. A., Xie, J., & Aldabbas, H. (2023). Privilege escalation attack detection and mitigation in cloud using machine learning. *IEEE Access*, *11*, 46561-46576.

[11]. Janabi, A. H., Kanakis, T., & Johnson, M. (2022). Overhead reduction technique for software-defined network based intrusion detection systems. *IEEE Access*, *10*, 66481-66491.

[12]. Mukesh Madanan, N. Muthukumaran, Shrikant Tiwari, A. Vijay & Indranil Saha, 'RSA based improved YOLOv3 network for segmentation and detection of weed species', Multimedia Tools and Applications, Volume 83, pages 34913–34942, 2024.

[13]. Vignesh. R, Muthukumaran. N, Philip Austin. M, 'Hybrid ResNet with Bidirectional LSTM for Eye Disease Classification with Evaluation Optimizers Techniques', International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, 2023, pp. 1624-1630.

[14]. Nallakaruppan, M. K., Somayaji, S. R. K., Fuladi, S., Benedetto, F., Ulaganathan, S. K., & Yenduri, G. (2024). Enhancing security of host-based intrusion detection systems for the internet of things. *IEEE Access*, *12*, 31788-31797.

[15]. Salman, T., Bhamare, D., Erbad, A., Jain, R., & Samaka, M. (2017, June). Machine learning for anomaly detection and categorization in multi-cloud environments. In *2017 IEEE 4th international conference on cyber security and cloud computing (CSCloud)* (pp. 97-103). IEEE.