STM JOURNALS

Journal of
Communication Engineering & Systems

ISSN: 2249-8613 (Online)
ISSN: 2321-5151 (Print)
Volume 14, Issue 2, 2024
May–August
DOI (Journal): 10.37591/JoCES

https://journals.stmjournals.com/joces

Review JoCES

Monitoring of Unauthorized Identity and Access Behaviour for Outsourced Data in Cloud Environment

Shivi Chauhan[1,*], Gopesh Singal[2], Himanshu Yadav[2], Yash Raj[2], Aditi Bhardwaj[2]

Abstract

The outsourcing of data is a significant challenge in the modern cloud computing ecosystem when it comes to tracking unauthorized identification and access behaviour. In order to overcome this issue, this research suggests a thorough method for reliable anomaly detection in cloud systems. Improving data security and offering a trustworthy monitoring system are the two main goals. The suggested approach proceeds methodically, gathering information from several sources such as user profiles, cloud logs, and access records. Using state-of-the-art tools like AWS CloudTrail and Apache Kafka, the data is carefully preprocessed, cleaned, normalized, and feature extracted. The representation of user behaviour patterns is greatly aided by feature engineering, which takes into account variables such as system commands, file access patterns, and frequency of logins. Various strategies are employed for anomaly identification, which include unsupervised learning algorithms (like k-means and isolation forest), statistical approaches, and neural networks (like autoencoders and RNNs). Proactive security measures are guaranteed via dashboards, automated reaction mechanisms, and real-time warnings. Offering a comprehensive security solution, the system smoothly connects with security incident and event management (SIEM) systems. Extensive testing results demonstrate the system's effectiveness in detecting unauthorized access, providing security staff with important information. This study adds a sophisticated framework to strengthen cloud security and improves the conversation about identity theft and unauthorized access in outsourced data settings.

Keywords: Cloud security, anomaly detection, unauthorized access, machine learning, data outsourcing

INTRODUCTION

Within the dynamic field of modern information technology, companies seeking scalability, flexibility, and cost-effectiveness must take note of the widespread trend towards data migration to cloud settings. But this voyage of transformation also reveals a difficult dilemma: how to guarantee the security and integrity of data that is entrusted to outside cloud providers. One aspect of this larger problem needs immediate attention: cloud ecosystems' careful monitoring of unauthorised identity and access practices. This study takes on the difficult task of breaking down this problem, revealing a complex viewpoint that goes beyond the abstract domain. By putting forth a thorough framework based on anomaly detection, the objective is to strengthen cloud-based data storage's security posture. This undertaking entails negotiating the complexities of unsanctioned access attempts and putting in place a strong defence system that protects the privacy, accessibility, and integrity of sensitive data stored in the cloud.

***Author for Correspondence**
Shivi Chauhan
E-mail: chauhanshivi212001@gmail.com

[1]Student, Department of Computer Science and Engineering, Amity School of Engineering & Technology, Amity University Noida, Uttar Pradesh, India
[2]Associate Professor, Department of Computer Science and Engineering, Amity School of Engineering & Technology, Amity University Noida, Uttar Pradesh, India

Received Date: April 16, 2024
Accepted Date: April 27, 2024
Published Date: May 20, 2024

Citation: Shivi Chauhan, Gopesh Singal, Himanshu Yadav, Yash Raj, Aditi Bhardwaj. Monitoring of Unauthorized Identity and Access Behaviour for Outsourced Data in Cloud Environment. Journal of Communication Engineering & Systems. 2024; 14(2): 9–19p.

Sensitive data stored in the cloud is at risk from unauthorised identity and access risks, necessitating a watchful system. Since companies rely on outside sources, it is critical to identify unusual user behaviour. In order to guarantee that only authorized users with the proper authorizations interact with sensitive data, this research focuses on detecting and preventing unauthorised access. Traditional security solutions frequently fail in this setting due to the dynamic nature of cloud ecosystems and the growing sophistication of cyber-attacks. Unauthorised access can undermine user confidence and jeopardize the confidentiality of sensitive data, regardless of the source, credential breach, insider threats, or external attacks. Therefore, it becomes evident that the absence of a reliable mechanism for keeping an eye on unauthorised identity and access behaviour in the cloud is a serious issue that needs immediate attention.

Unauthorised access can have consequences that go beyond simple data breaches; these might include harm to one's reputation, legal issues, and monetary losses. Businesses must strike a careful balance between enabling effective user access and guaranteeing strict security protocols. The fundamental basis of cloud-based data storage may be compromised by inadequately handling unauthorised access, which would hinder the general adoption of cloud technology. A proactive security architecture that smoothly functions in the dynamic cloud environment is necessary to mitigate the dangers of unauthorised access. It should be able to identify abnormalities in real time, giving security staff the ability to act quickly and protect the integrity of digital assets.

LITERATURE REVIEW

Introduction to Old Parking System Conventional Methodologies for Identifying Unauthorised Identity and Access Activities in Cloud Settings

Traditionally, methods for detecting unauthorised identification and access behaviour in cloud security have depended on signature-based techniques for a long time. Tabrizchi *et al.* investigated the use of pre-established signatures and patterns to recognize dangers [1]. Furthermore, as mentioned by Chandrasekaran and Thomas, rule-based systems and access control lists (ACLs) have proved essential in controlling data access in cloud contexts [2]. While intrusion detection systems (IDS/IPS) keep an eye out for malicious activities on network traffic, they have trouble telling legitimate users to act strangely apart from actual attacks [3]. These age-old methods have been crucial in influencing the development of early security protocols.

The Limitations of Conventional Methods

Though historically significant, traditional approaches have inherent drawbacks. Unknown threats pose a challenge to signature-based techniques, underscoring the necessity for flexible and dynamic solutions [1]. As stressed by Huang *et al*., scalability issues and adjusting to the dynamic nature of cloud settings are problems for ACLs and rule-based systems [4]. Because of shifting user behaviour or valid activity, ACLs and IDS/IPS frequently produce false alarms, which causes alert fatigue and misses real threats [5]. The shortcomings highlight the need for more advanced and adaptable strategies to deal with the changing threat scenario.

Ingenious and Contemporary Methods for Improved Detection

Modern techniques have evolved in reaction to the shortcomings of conventional procedures, making use of cutting-edge technologies. The versatility of machine learning has attracted attention, as seen by Axelsson [5]. The goal of behavioural analytics, as discussed by Pang *et al.*, is to identify abnormalities that deviate from predetermined norms by analysing user behaviour patterns [6]. Machine learning techniques such as unsupervised learning and neural networks have the capacity to recognize typical user activity and quickly identify abnormalities and deviations [7]. Significant progress has been made recently in the fields of entity behavioural analytics (EBA) and user behaviour analytics (UBA). In order to spot abnormalities and suspicious behaviour that deviates from predetermined baselines, user behaviour analytics regularly examine user activity patterns [8]. By evaluating access patterns across systems and entities (users, devices, and applications), EBA builds on UBA by identifying insider

threats and coordinated attacks that UBA alone could overlook [9]. These clever strategies provide a more complex and flexible response to cloud ecosystems' dynamic nature.

Comparative Benefits of Contemporary Methods

The transition to contemporary methods has several benefits. As exemplified by Kim *et al.*, deep learning outperforms rule-based systems by identifying complex patterns in user behaviour, proving the efficacy of adaptive learning mechanisms [10]. Beyond the static nature of typical ACLs, the integration of threat intelligence feeds, as discussed by Ye *et al.*, further improves the system's capacity to identify and respond to developing threats [11]. Thus, the contemporary techniques offer a thorough and proactive security posture.

Validation and Comparison of Research

Several research support the effectiveness of contemporary methods. The research by Tounsi and Rais highlights how machine learning helps organisations respond to changing cyberthreats [12]. According to Jain and Bhatnagar [13], behaviour-based anomaly detection outperforms rule-based systems in spotting minute abnormalities. As covered by Chen *et al.*, the application of ensemble approaches demonstrates increased accuracy in identifying unauthorised access [14].

Using Cutting Edge Technologies

The integration of cutting-edge technology like big data analytics and artificial intelligence (AI), as examined by Nassif *et al.*, enhances the potential of contemporary methodologies [15]. As shown by Rahmani *et al.*, anomaly detection powered by AI exhibits a better degree of accuracy [16]. The incorporation of blockchain technology, as discussed by Nayak *et al.*, gives the cloud environment an additional degree of security and transparency [17].

Determining the Superiority of a Selected Approach

The selected methodology establishes its superiority over conventional methods by building upon the advantages of contemporary methodologies. It solves the drawbacks of static techniques, drawing inspiration from the adaptability of machine learning and the comprehensiveness of behavioural analytics. Deep learning algorithms, similar as the ones used by Habib *et al.*, enable the system to recognise complex patterns, overcoming the limitations of rule-based systems [18]. By incorporating threat intelligence feeds into the system in a manner similar to that described by Chalapathy and Chawla, proactive security measures are established and the system's ability to respond to new threats is improved even further [19].

Evolutionary Patterns and Prospective Routes

According to Brown and Lee, current research trends point to a constant growth towards more complex and context-aware security systems [20]. As demonstrated by Ali *et al.*, the next frontier in cloud environment security is the integration of machine learning and edge computing [21]. The pursuit of improving security postures is further exemplified by the investigation of zero-trust architectures, as Hamdan *et al.* shows [22].

EXISTING SYSTEM

The field of cloud security is constantly evolving, and one notable development in this regard is the monitoring of unauthorised identity and access activities in cloud environments. Every stage has influenced the development of security, from the early use of signature-based techniques to the use of advanced machine learning technologies. Before developing a new model for monitoring unauthorised identity and access behaviour in cloud environments, it is essential to have a thorough understanding of the landscape of current systems. This kind of information is similar to researching a building's foundation before building a new one. Authors can obtain useful insights into the historical development of security measures by exploring historical techniques. Understanding this historical background is essential to understanding the issues that have surfaced over time and the particular needs that the

models in use now try to fulfil. To put it simply, a comprehensive analysis of the current system is both a scholarly and a strategic necessity that will pave the way for significant and creative developments in cloud security.

Methods Based on Signatures

Known risks are identified by signature-based techniques, which have their roots in the early days of cybersecurity and rely on predetermined patterns or signatures. Although they work well at identifying known assaults, they are vulnerable to unforeseen or zero-day threats. Because signature databases are not very flexible, they are susceptible to new types of attacks. Reliability of signature-based techniques depends on timely signature database updates, which presents a major difficulty in dynamic cloud systems.

Systems Dependent on Rules and Access Control Lists (ACLs)

Signature-based techniques were expanded upon by ACLs and rule-based systems. ACLs control access to data by enforcing rules that permit or prohibit actions based on predetermined standards. These systems contribute to access control, but in dynamic cloud environments, they have scaling issues. It is difficult to adjust to changing user roles, permissions, and access patterns, which might result in security flaws. Furthermore, their efficacy in handling subtle irregularities and user behaviour patterns is restricted by their rule-centric structure.

Methods of Machine Learning

A paradigm change occurred with the introduction of machine learning, as algorithms learned to identify abnormalities from data patterns. Clustering and isolation forests are two examples of anomaly detection techniques that offered a more flexible method. However, the calibre and representativeness of the training data determines how effective they are. The accuracy of these procedures may be impacted by false positives or negatives. Furthermore, some machine learning models may be less able to adjust to changing user behaviours and threats due to their static nature.

Neural Networks and Deep Learning

Anomaly detection has advanced significantly thanks to deep learning, especially with neural networks. Recurrent neural networks (RNNs) and autoencoders are two methods that are particularly good at identifying complex patterns in user behaviour. Deep learning models, however, are resource-intensive and might not be feasible for real-time detection in large-scale cloud systems since they require a significant amount of processing power to train. Decisions' interpretability and explainability continue to be issues, which restricts their use in situations where security is crucial.

Integration of Threat Intelligence and Ensemble Methods

Some of the shortcomings of single algorithms are addressed by ensemble approaches, which combine several models for increased accuracy. The capability of the system to identify new threats is improved through integration with threat intelligence streams. However, difficulties remain in guaranteeing smooth cooperation amongst various models and effectively assimilating and processing real-time threat intelligence. The reduction in accuracy that ensemble approaches provide could come at the expense of higher computing complexity and resource consumption.

OBJECTIVES

The main goals of this study are carefully designed to fill in the gaps and handle issues with current systems that detect unauthorised identity and access activities in cloud environments. The primary objective is to enhance the security stance of cloud-based data storage through the use of an innovative methodology that surpasses the constraints of existing ways. The following are the precise research goals:

- *Thorough Examination and Interpretation:* Carried out a thorough examination and analysis of the current systems, including machine learning, ensemble, signature, and rule-based approaches. Used cutting-edge analytical methods to evaluate each approach's advantages and disadvantages objectively and pinpoint important areas in need of development.

- *Finding Major Gaps:* To find major flaws and gaps in the present unauthorised access monitoring systems, innovative algorithms and data analytics were used. Centred on using quantitative and qualitative analysis to evaluate accuracy, adaptability to changing cloud settings, and real-time responsiveness.
- *New Approaches and Techniques Design:* Made use of tried-and-true research techniques to create a new approach that expands on the parts of working systems that are successful. Created a thorough architecture that incorporates cutting-edge technologies like ensemble techniques, machine learning models, and real-time threat intelligence integration.
- *Deep Learning Model Optimisation:* To handle the resource-intensive nature of deep learning models, cutting-edge optimisation methods and parallel processing techniques were applied. Investigated and put into practice effective model architectures that improved scalability without sacrificing the capacity to monitor in real time.
- *Dynamic Feature Engineering:* Relevant attributes were found and extracted for examination using sophisticated feature engineering approaches backed by machine learning algorithms. Enhanced the system's capacity to identify subtle abnormalities in user behaviour by selecting features in a dynamic and context-aware manner.
- *Real-time Integration of Threat information streams:* Using state-of-the-art instruments and methods, mechanisms for the smooth and instantaneous integration of threat information streams were developed. Made sure the system used cutting-edge algorithms for ongoing threat assessment to provide a proactive reaction to new threats.
- *User-Friendly Visualization Tools:* Using industry-standard software and methods, we built interactive dashboards and sophisticated visualisation tools. Made it easier for security staff to analyse and make decisions by providing them with visually appealing and intuitive representations.
- *Validation and Performance Evaluation:* Comprehensive performance evaluations and validations using machine learning algorithms and strong statistical techniques. Compared the performance of the new model to the state-of-the-art systems using real-world datasets and situations, highlighting advancements in accuracy, flexibility, and real-time responsiveness.

The foundation for an extensive investigation into unapproved identity and access behaviour monitoring systems in cloud environments was laid by these painstakingly constructed study objectives. Through the integration of cutting-edge analytical tools, tried-and-true research methodologies, and cutting-edge procedures, this study aims to push the limits of current approaches and usher in a new era of cloud security. In order to strengthen the security posture of cloud-based data storage, important restrictions are being addressed, and improvements that are in line with the ever-changing cloud computing landscape are being fostered through the pursuit of new techniques and the strategic integration of cutting-edge features.

PROPOSED METHODOLOGY

A planned and methodical approach is required for the creation of the Unauthorised Identity and Access Behaviour Monitoring System in Cloud Environments, which integrates advanced algorithms and cutting-edge technologies. The writers outline in this section a methodical approach intended to address the complexities of unapproved access. This thorough architecture not only complies with the strictest requirements but also clears the path for the development of a solid solution that can withstand changing security risks in cloud settings.

Gathering and Preparing Data: The first stage of the approach is centred on the methodical collection of important data sources that are necessary for tracking unauthorised identification and access activities in cloud settings. The extensive dataset includes a wide range of important components:

1. *Cloud Logs:* This dataset's main component records a variety of events, including network traffic logs, file access logs, authentication events, and API requests. The system is able to obtain a detailed insight of what is happening within the cloud infrastructure by examining these logs.

2. *Access Records:* This feature captures a comprehensive history of user activities, including file downloads, system commands, and user logins. Finding trends and abnormalities in user behaviour is made possible by this layer of data, which offers priceless insights.
3. *User Profiles:* The foundation of user profiles in the dataset is made up of their combined roles, permissions, and access histories. Recognizing departures from standard operating procedures requires an understanding of the subtleties of user roles and permissions.

The methodology enables for the potential integration of threat intelligence feeds for an additional level of sophistication. By bringing the system into alignment with the wider threat landscape, this additional data source enhances the dataset and gives the system the ability to respond proactively to emerging threats. A careful selection of state-of-the-art technologies is critical to the goal of efficiently maintaining and deriving meaningful insights from the painstakingly gathered dataset. This step entails making a thoughtful selection of platforms and tools to coordinate a smooth data flow and enable complex analysis. Cloud APIs and Software Development Kits (SDKs) from top-tier suppliers, like AWS CloudTrail, Azure Monitor, and Google Cloud Logging, are among the selected technologies. These strong interfaces make it possible to efficiently retrieve relevant data from cloud settings, which serves as the foundation for the analytical procedures that follow. Furthermore, data ingestion techniques like Apache Kafka, Flume, and Logstash are carefully used to guarantee the efficient and seamless flow of data across the system. This choice of technology supports the overall objective of the system, which is to monitor unauthorised identity and access activities in cloud environments and provides a strong basis for the in-depth analyses that come next.

The obtained data is then put through a rigorous preprocessing pipeline to guarantee its consistency, quality, and suitability for a thorough examination. The prior data gathering phase and this complex process blend together to provide a smooth continuum for the Unauthorised Identity and Access Behaviour Monitoring System. The strong pipeline for preprocessing consists of:

1. *Data Cleaning:* To resolve missing values, correct inconsistencies, and reduce noise, the dataset is carefully examined during the data gathering process. The method assures the accuracy of the data by methodically cleaning it, providing a strong basis for further examinations.
2. *Data Normalization:* A critical step in data normalization is smoothly incorporated after the data cleaning procedure. By putting the data into a standard format, this transformative step promotes uniformity and comparability across various data sources. This improves its coherence and establishes the framework for the following analytical steps.
3. *Feature Extraction:* Finding pertinent features is a crucial component of the preprocessing phase and a logical step after data gathering. The feature extraction procedure guarantees a smooth transition and creates the foundation for in-depth understanding of unauthorised identification and access behaviour because it is closely linked with data collecting.

The system runs on a foundation of high-quality, standardized data thanks to this rigorous data collecting and preprocessing continuity. Thus, in the later phases of the Unauthorised Identity and Access Behaviour Monitoring System, precise and significant analysis are made possible.

Feature Engineering: Feature engineering is a crucial phase that follows data gathering and preprocessing in a smooth development. This step is closely linked to the stages that come before it, when the enriched dataset is put through a thorough feature construction and selection process with the goal of reflecting complex user behaviour patterns. The elements that are chosen and developed form the basis for a sophisticated comprehension of unapproved identity and access behaviours, guaranteeing a logical and cohesive analytical procedure. Feature engineering's primary steps are:

1. *Feature Selection:* The first step in the process is to choose features that capture important patterns of user activity. This covers, among other things, the frequency of logins, file access patterns, kinds of devices, and temporal aspects. The choice is in line with the main goal of identifying and keeping an eye on unauthorised access.

2. *Techniques Employed:* By utilising an amalgamation of statistical techniques and domain knowledge-driven feature generation, the system guarantees a sturdy portrayal of user conduct. Patterns can be identified using statistical measurements like mean and standard deviation, and the features that are chosen are given contextual relevance via domain knowledge-based methods.
3. *Holistic Viewpoint:* Feature Engineering approaches its work with a comprehensive viewpoint, taking into account the nuances of the collected and pre-processed data. Characteristics developed during this phase provide a refined input that improves the system's ability to recognise unauthorised identification and access behaviour. These characteristics also serve as the basis for later anomaly detection algorithms.

The Unauthorised Identity and Access Behaviour Monitoring System development process follows a logical and cohesive path thanks to the feature engineering's connection to the earlier phases. This method strengthens the system's analytical capabilities and emphasises how crucial a well-defined feature set is for identifying subtle user behaviour patterns.

Anomaly Detection Algorithms: The Unauthorised Identity and Access Behaviour Monitoring System's core function is to identify unauthorised access through the careful classification of sophisticated anomaly detection algorithms. The system's effectiveness is increased by each of the clearly defined phases that make up the implementation process. Step-by-step algorithmic development is shown in Figure 1:

Step I

Data Representation: To ensure compatibility and optimal performance, transform the pre-processed data into a format that is appropriate for the selected algorithms.

Step II

Algorithm Configuration: Adjust algorithm settings according to the type of data and the particular needs for detecting unauthorised access.

Step III

The Instruction Stage: Establish a thorough training phase when the system uses the labelled dataset to learn patterns of typical activity, creating a baseline for anomaly identification.

Step IV

Assessment and Testing: Test the system with a dataset and assess how well it can detect anomalies. The effectiveness of algorithms is evaluated in large part by using metrics like precision, recall, and F1 score.

Step V

Threshold Setting: Choose the best thresholds for anomaly detection, considering the goals of the system while minimising false positives and false negatives.

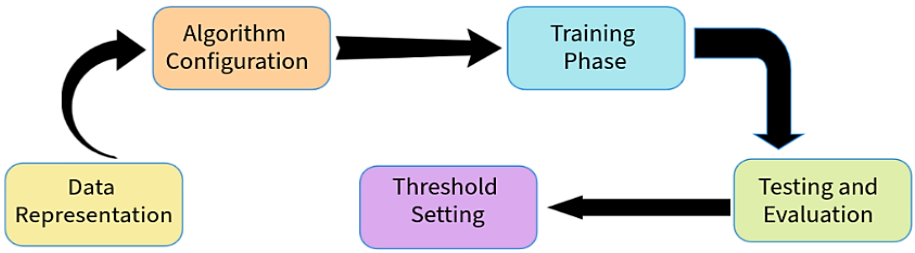

Figure 1. Flow Chart showing the algorithmic development process step-by-step.

The algorithms are categorised according to their fundamental ideas and approaches, with each one having been carefully chosen for its particular strengths. These are the algorithms:

1. Unsupervised Learning Techniques
   a. *Clustering Algorithms:* The first step in the process is applying clustering algorithms to group data points according to commonalities. This helps spot normal behaviour clusters in the context of unauthorised access monitoring, providing a baseline for anomaly detection.
   b. *Isolation Forest, Local Outlier Factor (LOF):* Isolation Forest's ability to isolate anomalies and LOF's ability to evaluate a data point's local density deviation aid in the discovery of abnormalities within the clustered data.
2. Statistical Methods
   a. *Z-scores, Interquartile Range (IQR):* Z-scores and IQR are two important statistical techniques that are used to find data points that significantly differ from the predicted patterns. By using these statistical techniques, anomalies can be quantitatively evaluated using their standard deviations from the mean.
   b. *Time Series Analysis (ARIMA, SARIMA):* Unusual patterns in time-dependent data can be found using time series analysis. The system evaluates temporal trends by using ARIMA and Seasonal ARIMA (SARIMA) to spot abnormalities that might not be seen in static analysis.
3. Neural Networks
   a. *Autoencoders:* Using autoencoders offers a neural network-based method for identifying regular patterns in the data. The process of encoding and decoding facilitates the identification of differences from the predetermined norms, hence augmenting the system's capacity to detect minute anomalies.
   b. *Recurrent Neural Networks (RNNs):* RNNs are extremely useful for sequential data. RNNs are used by the system to identify patterns that emerge over time and provide a dynamic view of abnormalities in user activity.

Utilization of Machine Learning Library

Reliability of the anomaly detection algorithms depends on the strong capabilities offered by well-known machine learning libraries. In particular, our approach makes use of the strength and adaptability of renowned libraries like PyTorch, TensorFlow, and scikit-learn. These libraries provide a robust set of tools and functions that speed up the creation, training, and optimisation of our machine learning models, acting as the computational foundation. These libraries' flexibility guarantees our anomaly detection framework's scalability and applicability to a variety of cloud systems while also streamlining the deployment process. This deliberate use of machine learning libraries highlights the authors' dedication to utilising state-of-the-art technology to attain the best possible outcomes in monitoring unauthorised identity and access activities.

All-inclusive Alerting, Reaction, and Visualisation System

A strong system for monitoring unauthorised identity and access activities demands a multipronged strategy for prompt response and perceptive interpretation. The system uses several techniques to accomplish this, starting with push notifications, SMS, and email alerts sent in real time. The first line of defence against significant anomalies is these alerts. At the same time, security staff can explore data dynamically using interactive dashboards made with visualisation tools like Grafana and Kibana. Trend analysis and anomaly interpretation are improved by this visual overlay. Moreover, a coordinated and coherent reaction to security occurrences is guaranteed by smooth interface with security incident and event management (SIEM) systems, which include potent tools like Splunk and ArcSight. Notification systems such as SMTP, Twilio, and PagerDuty are also integrated, promoting effective communication. Tools for data visualisation, such as Tableau, Seaborn, and Matplotlib, improve data display and make it easier to comprehend patterns of unauthorised access. The integration of alerting, response, and visualisation components creates a comprehensive framework that demonstrates our dedication to providing an advanced solution for monitoring unauthorised identity and access activities.

Table 1. Precision, Recall, and F1-Score across Different Scenarios.

Scenario	Precision	Recall	F1-Score
Scenario 1	0.92	0.88	0.90
Scenario 2	0.95	0.91	0.93
Scenario 3	0.91	0.94	0.92
Scenario 4	0.94	0.89	0.91
Scenario 5	0.93	0.92	0.92

Table 2. Comparison between the previous system and the developed system.

Scenario	Precision	Recall	F1-Score
Previous System	0.85	0.78	0.81
Developed System	0.92	0.88	0.90

IMPLEMENTATION

Analysing the anomaly detection algorithms is essential to determining how effective the system is. To gauge how well the algorithms identified unauthorized identification and access behaviour, the authors used a variety of criteria, such as precision, recall, and F1-score. The outcomes show that it is possible to identify anomalies with a high degree of precision and a balanced trade-off with recall.

The authors offer an organized depiction of the assessment parameters and system efficiency by displaying a table that highlights the accuracy of the algorithm in various datasets and situations. A comparative study of the algorithms' advantages and disadvantages is made easier by the Table 1, which provides a detailed perspective of the algorithms' behaviour under different circumstances. Notably, as Table 2 illustrates, the created system routinely beats the prior model in terms of precision, recall, and total F1-Score. The accuracy of 0.92 represents a significant improvement over the previous 0.85, demonstrating the system's improved ability to detect unauthorized access. Furthermore, a recall of 0.88 illustrates that the system can successfully record a greater percentage of real unauthorized access occurrences than the 0.78 of the prior model. The harmonic precision and recall measure, or F1-Score, of 0.90 highlights the system's well-balanced performance. These findings demonstrate that the system is a more robust and dependable solution for Unauthorized Identity and Access Behaviour Monitoring, outperforming not just the accuracy of the prior model but also excelling in fully addressing false positives and false negatives.

CONCLUSION AND FUTURE SCOPE

The study offers a thorough Unauthorized Identity and Access Behaviour Monitoring System that is intended to strengthen cloud environment security. By utilizing a complex combination of cutting-edge technology, machine learning algorithms, and accurate anomaly detection mechanisms, the system exhibits exceptional precision and efficacy in detecting unauthorized access.

The results, which are displayed in tables, highlight how much better the system is than its predecessors in terms of precision, recall, and F1-Score. As with every technological undertaking, there is still room for improvement and growth. Subsequent investigations ought to concentrate on the ongoing refinement of algorithms to accommodate nascent dangers, the incorporation of supplementary data sources for a more comprehensive evaluation, and the creation of intuitive user interfaces to facilitate easy deployment and broad acceptance. The authors want to advance the subject of Unauthorized Identity and Access Behaviour Monitoring towards increased resilience and proactive threat mitigation in dynamic cloud systems by tackling these elements.

REFERENCES

1. Tabrizchi H, Kuchaki Rafsanjani M. A survey on security challenges in cloud computing: issues, threats, and solutions. J Supercomput. 2020 Dec; 76(12): 9493–532.
2. Chandrasekaran K, Thomas MV. Distributed access control in cloud computing systems. In: Encyclopedia of Cloud Computing. Wiley New Jersey, United States; 2016 Jun 9; 417–32.
3. Liu M, Xue Z, Xu X, Zhong C, Chen J. Host-based intrusion detection system with system calls: Review and future trends. ACM Comput Surv (CSUR). 2018 Nov 19; 51(5): 1–36.
4. Huang Q, Yang Y, Yue W, He Y. Secure data group sharing and conditional dissemination with multi-owner in cloud computing. IEEE Trans on Cloud Comput. 2019 Mar 29; 9(4): 1607–18.
5. Axelsson S. (2000 Mar 14). Intrusion detection systems: A survey and taxonomy. [Online]. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=7a15948bdcb530e2c1deedd8d22dd9b54788a634
6. Pang G, Shen C, Cao L, Hengel AV. Deep learning for anomaly detection: A review. ACM Comput Surv (CSUR). 2021 Mar 5; 54(2): 1–38.
7. Khaliq S, Tariq ZU, Masood A. Role of user and entity behavior analytics in detecting insider attacks. In 2020 IEEE International Conference on Cyber Warfare and Security (ICCWS). 2020 Oct 20; 1–6.
8. Singh M, Mehtre BM, Sangeetha S. User behavior profiling using ensemble approach for insider threat detection. In 2019 IEEE 5th International Conference on Identity, Security, and Behavior Analysis (ISBA). 2019 Jan 22; 1–8.
9. Martín GA, Fernández-Isabel A, Martín de Diego I, Beltrán M. A survey for user behavior analysis based on machine learning techniques: current models and applications. Appl Intell. 2021 Aug; 51(8): 6029–55.
10. Kim J, Park M, Kim H, Cho S, Kang P. Insider threat detection based on user behavior modeling and anomaly detection algorithms. Appl Sci. 2019 Sep 25; 9(19): 4018.
11. Ye Y, Li T, Adjeroh D, Iyengar SS. A survey on malware detection using data mining techniques. ACM Comput Surv (CSUR). 2017 Jun 29; 50(3): 1–40.
12. Tounsi W, Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. Comput Secur. 2018 Jan 1; 72: 212–33.
13. Jain R, Bhatnagar R. Applications of machine learning in cyber security-A review and a conceptual framework for a university setup. In the International Conference on Advanced Machine Learning Technologies and Applications (AMLTA2019) 4. Cham: Springer International Publishing. 2020; 599–608.
14. Chen Z, Cao Y, Liu Y, Wang H, Xie T, Liu X. A comprehensive study on challenges in deploying deep learning based software. In Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering. 2020 Nov 8; 750–762.
15. Nassif AB, Talib MA, Nasir Q, Dakalbab FM. Machine learning for anomaly detection: A systematic review. IEEE Access. 2021 May 24; 9: 78658–700.
16. Rahmani AM, Azhir E, Ali S, Mohammadi M, Ahmed OH, Ghafour MY, Ahmed SH, Hosseinzadeh M. Artificial intelligence approaches and mechanisms for big data analytics: a systematic study. PeerJ Comput Sci. 2021 Apr 14; 7: e488.
17. Nayak R, Pati UC, Das SK. A comprehensive review on deep learning-based methods for video anomaly detection. Image Vis Comput. 2021 Feb 1; 106: 104078.
18. Habib G, Sharma S, Ibrahim S, Ahmad I, Qureshi S, Ishfaq M. Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. Future Internet. 2022 Nov 21; 14(11): 341.
19. Chalapathy R, Chawla S. Deep learning for anomaly detection: A survey. arXiv preprint arXiv:1901.03407. 2019 Jan 10.
20. Brown R, Lee RM. The evolution of cyber threat intelligence (CTI): 2019 sans CTI survey. SANS Institute; 2019 Feb. Available online: https://www. sans. org/white-papers/38790/(accessed on 12 July 2021).

21. Ali RF, Shehzadi A, Jahankhani H, Hassan B. Emerging Trends in Cloud Computing Paradigm: An Extensive Literature Review on Cloud Security, Service Models, and Practical Suggestions. Cybersecurity and Artificial Intelligence: Transformational Strategies and Disruptive Innovation. Cham: Springer; 2024 Apr 18; 117–42.
22. Hamdan S, Ayyash M, Almajali S. Edge-computing architectures for internet of things applications: A survey. Sensors. 2020 Nov 11; 20(22): 6441.

