AI and Machine Learning Advances
Volume 2, Issue 2
ISSN: 3067-3216

AI-Driven Threat Modeling for Identity and Access Management in Multi-Tenant Clouds

[1]*Dinesh Kollu
[1]Department of Engineering, Madras University, India.

Abstract

The high rate of Cloud computing and multi-tenant architectures adoption has greatly complicated Identity and Access Management (IAM) systems security. Conventional rule-based access control systems can be very difficult to detect misconfigurations and threats that emerge in dynamic clouds. The study provides an artificial intelligence-based discussion of an IAM security setup to establish the key attributes that affect access control security in multi-tenant cloud environments. The dataset that consisted of 100,000 IAMs with 50 parameters that reflect the security level was examined to determine the predictability of the machine learning in predicting the security strength. The data set contains authentication mechanisms, authorisation models, governance frameworks and network security control with a security score as the target variable. To model the link between the IAM parameters and the security scores, a Random Forest classifier was used. The experimental findings indicate that the suggested method works with an accuracy of 82.6 per cent in forecasting IAM security settings. In the analysis of the feature importance, it is possible to identify user identity management, access levels, data governance frameworks, geolocation restrictions, and access control by tokens as some of the most powerful security factors. The results indicate the relevance of tiered security features that entail a combination of identity checks, policy controls, and network defence. The study can be used to design AI-based threat modelling and mitigation strategies that enhance IAM security in multi-tenant cloud system applications.

Keywords: AI-driven cloud security, Identity Access Management, multi-tenant cloud environments, machine learning cybersecurity, access control security, cloud threat detection.

1. Introduction

1.1 Background

Cloud computing now forms an essential part of the contemporary digital infrastructure and allows organisations to implement scalable, flexible, and cost-effective computing capabilities. The large-scale use of cloud technologies has increased the pace of implementation of multi-tenant cloud architecture in which different users or organisations share the same computing infrastructure without physically sharing resources. Inasmuch as such an architecture enhances efficiency and the use of resources, it also poses major security threats, especially when it comes to the administration of identities and access privileges (Kumar, 2022; Yadav & Abidin, 2025). Assuring safe access to cloud resources is thus a crucial issue of concern to organisations that use the cloud application to handle sensitive information and mission-critical applications.

Identity and Access Management (IAM) is an important component of cloud environment protection as it regulates the interaction of users with cloud resources and their authentication. It is common to find IAM structures that have authentication functionalities, authorisation designs, role-based access controls, and policy enforcement engines that identify which users are allowed to access certain resources (Abdiukov, 2025; Hariharan, 2025b). Proper IAM systems also mean that only authorised users have access to sensitive information and cloud services, and this minimises the chances of any data breach and unauthorised access. But with the growth of cloud environments, the traditional IAMs are severely constrained in dealing with the emerging cyber threats.

There are various categories of security threats to cloud IAM systems. These are privilege escalation attacks, unauthorised access, identity spoofing, and policy misconfigurations that might allow unscrupulous parties to access sensitive resources (Naeem, 2023; Tripathi, 2023). User-based attacks and hacks can also exacerbate the probability of security violations in multi-tenant

Dinesh Kollu
Department of Engineering, Madras University, India.
Email: kolludinesh1@gmail.com

Received: 26-Mar-2026 Revised: 20-April-2026 Accepted: 29-April-2026

AI and Machine Learning Advances
Volume 2, Issue 2
ISSN: 3067-3216

environments. The dynamism of cloud infrastructures is such that the traditional mechanisms of security cannot effectively detect and respond to such threats. Consequently, scholars and professionals are turning to artificial intelligence (AI) and machine learning solutions as new and enhanced solutions to enhance cloud security (Abbas & Myeong, 2023; Helina, 2025).

Machine learning techniques have been shown to hold a lot of promise in predicting security threats, anomaly detection, and enhanced automated decision-making in cloud environments. An AI-based security model can detect the patterns indicating that the system may be vulnerable or demonstrating suspicious behaviour by analysing extensive amounts of system logs and security settings (Al-Ghuwairi et al., 2023; Bhaskaran & Achar, 2025; Olabanji et al., 2024). These technologies can be used to detect threats in advance and also to help organisations implement adaptive security strategies that keep up with the new threats. As a result, AI-assisted security systems are becoming an integral element of new cloud security systems.

1.2 Problem Statement

Although the role of the IAM systems in cloud security is becoming increasingly significant, most of the available solutions continue to depend on fixed, rule-based policies and predefined models of access control. Such conventional mechanisms can frequently not be enough in the recognition of both complex and dynamic security risks in advanced cloud setups. Manually defined security policies are common in rule-based systems, which can not keep up with changing attack patterns or misconfigurations in large-scale cloud systems (Goyal, 2025; Saxena et al., 2023). As the multi-tenant cloud platforms become more and more complex, it becomes hard to keep track of and deal with the access control settings in a traditional manner. The other problem is the large number of security parameters of IAM settings. Clouds involve various access controls, including authentication policies, authorisation policies, encryption policies, governance policies, and network security policies. These parameters are time-consuming and prone to errors when analysed manually in order to determine the risk of security. Consequently, organisations need smart systems that would automatically inspect the IAM settings and detect possible vulnerabilities before they can be exploited by attackers (Polu, 2025).

1.3 Research Objective

- Develop a machine learning model of threat modelling in Identity and Access Management (IAM) systems in multi-tenant clouds.
- Predict cloud access control settings through machine learning to determine the major parameters influencing IAM security.
- Develop predictive modelling to identify security risks and access control misconfigurations that enhance the overall management of clouds.

1.4 Research Contributions

This study has a number of contributions to the practice of cloud security and identity management. It suggests that an AI-based taxonomy of IAM threats that types the frequent vulnerabilities and security risks found in the multi-tenant cloud environment. The study provides a thorough study of the parameters of the cloud access control based on a massive dataset that comprises various IAM security features. Machine learning models are deployed that forecast the level of security risks according to the information of IAM configuration and show the possibility of AI-based solutions for proactive threat detection. The research suggests mitigation measures that help to increase security on IAM and decrease the risk of unauthorised accessibility in the cloud-based environment. These articles can serve as important information on the design of intelligent security systems that can help build safer and more robust cloud systems (Cheruku, 2025; Pujari, 2025).

2. Methodology

This study uses a machine learning approach based on data analysis to examine Identity and Access Management (IAM) settings and detect security threats within a multi-tenant cloud architecture. The methodology framework includes: dataset selection, data preprocessing, model development and performance evaluation. The goal of this methodology is to design predictive models that are able to analyse the access control setup and identify the possible security risk situations in cloud structures.

2.1 Dataset Description

The research employs the Cloud Access Control Parameter Management Dataset that comprises several parameters that express IAM security configurations on clouds. The dataset is modelled after the environment of access control that is typically employed in cloud

infrastructures and offers an organised illustration of authentication schemes, authorisation patterns, policy-enforcing regulations, and control measures.

The data comprises about 100,000 records and 50 security-related features, and a target variable that indicates the overall security rating of the access control setup. Every record represents a distinct IAM setup comprising various security controls and access management settings.

There are many types of IAM security features covered in the dataset. Authentication features are those elements that are involved in authenticating the user identity, like password-based authentication, biometric authentication, or multi-factor authentication. Parameters to do with authorisation detail the manner in which access permissions are granted and enforced with models like role-based access control (RBAC), attribute-based access control (ABAC) and privilege management mechanisms. The identity management features are identity verification, identity federation and identity lifecycle management processes.

Besides identity-related parameters, network security controls that the dataset contains are geolocation limitations, firewall rules, and virtual private network settings. The monitoring and governance aspects are also added to manifest audit logging, compliance enforcement, and security policy management. All these features present a very detailed picture of the IAM configurations and their possible effect on the security of the cloud.

Machine learning prediction is on the Security Score variable as the target variable. This variable is the total security of the access control configuration, and it is to be used to train predictive models that are able to recognise risky configurations.

2.2 Data Preprocessing

Preprocessing the dataset before training the machine learning models involves a series of processes that guarantee the quality of data and enhance the models by enhancing their performance. Preprocessing of data is an important step in the analysis of machine learning before processing other raw data.

The initial one is the data cleaning process that implies the verification of missing or conflicting values in the dataset. All missing values are dealt with using relevant strategies to make sure that incomplete records do not impact the process of training a model.

The second step includes coding categorical variables. A large number of IAM features, like authentication mechanisms, authorisation models, and user roles, are in the form of categorical values. Encoding methods are used to transform these categorical features into numerical forms in order to become subject to machine learning algorithms.

The third preprocessing procedure is feature normalisation and transformation. Numerical characteristics are normalised to achieve similar values across the data. Normalisation is used to avoid the dominance of features whose numerical values are large in the learning algorithm and enhances the stability of machine learning models.

The last step of preprocessing is the feature selection and preparation of dimensionality. The IAM security parameters are stored in a relevant manner to make sure that the machine learning models are concerned with relevant security-related attributes. The data is then split into a training and testing set so that the models can learn from previous historical data and test their predictive accuracy on previously unknown configurations.

2.3 Machine Learning Models

A number of trained machine learning algorithms are used to process the data available on IAM configuration and give findings on the security score of each configuration. Such models are chosen considering their efficiency in the classification activity and their capacity to address complicated relationships between security parameters.

Random Forest algorithm is the main classification model applied because it is powerful and capable of dealing with high-dimensional data. Random Forest builds more than one decision tree, and it integrates the predictions of the trees in order to enhance the accuracy of classification and reduce overfitting.

The Support Vector Machine (SVM) model is also applied to carry out the classification by determining the best decision boundaries among various classes of security scores. SVMs work best with data sets that have complicated interactions of features.

The XGBoost algorithm is used as a gradient boosting model that recursively constructs decision trees in order to reduce errors in prediction. XGBoost is famous due to its efficiency and good predictive abilities on structured data.

These models are developed on the preprocessed data to train the relation between IAM security parameters and the security score.

2.4 Evaluation Metrics

In determining the effectiveness of the machine learning models, a number of evaluation metrics are applied. These metrics offer an all-around evaluation of the

AI and Machine Learning Advances
Volume 2, Issue 2
ISSN: 3067-3216

classification performance and predictive excellence of the models.

Accuracy is a measure of the general percentage of cases in the dataset which have been correctly classified. It gives an overall measure of the model's performance.

Precision determines the percentage of the correctly predicted positive cases of all the predicted positive cases. This measure is especially crucial to consider the quality of predictions of threat detections.

Recall is a ratio of true positive cases that the model responds to correctly. The high recall means that the model is effective in identifying security risks.

F1-score is a harmonic mean of recall and precision and is a balanced metric of model performance when there is an imbalanced dataset.

The Receiver Operating Characteristic-Area under the Curve (ROC-AUC) measure is a measure of the model in terms of its capacity to differentiate the various scores of security based on its various classification levels.

The metrics of the evaluation are utilised to compare the work of the implemented machine learning models and determine whether they are effective in predicting the IAM security risks in cloud environments.

3. Results

The findings of the analysis of the Identity and Access Management (IAM) data, which is an experiment under machine learning. The aim of the experiments was to determine whether machine learning models can examine cloud access control settings and estimate the security of IAM policies. The data that was used in this study is 100,000 IAM configurations consisting of 50 security-related parameters and a security score as a label that is the target variable to classify.

3.1 Security Score Distribution

The distribution of the security score in the dataset was studied using an initial exploratory analysis. The security scores are distributed as shown in Figure 1. The findings indicate that most of the settings score 4, which is a moderately secure IAM setting. The smaller part of the records is included in the category of security scores of 3, with very few settings corresponding to extremes of 2 and 5.

This distribution shows that the majority of the IAM setups in the dataset use only standard security controls and might not have all the sophisticated security measures. The dataset

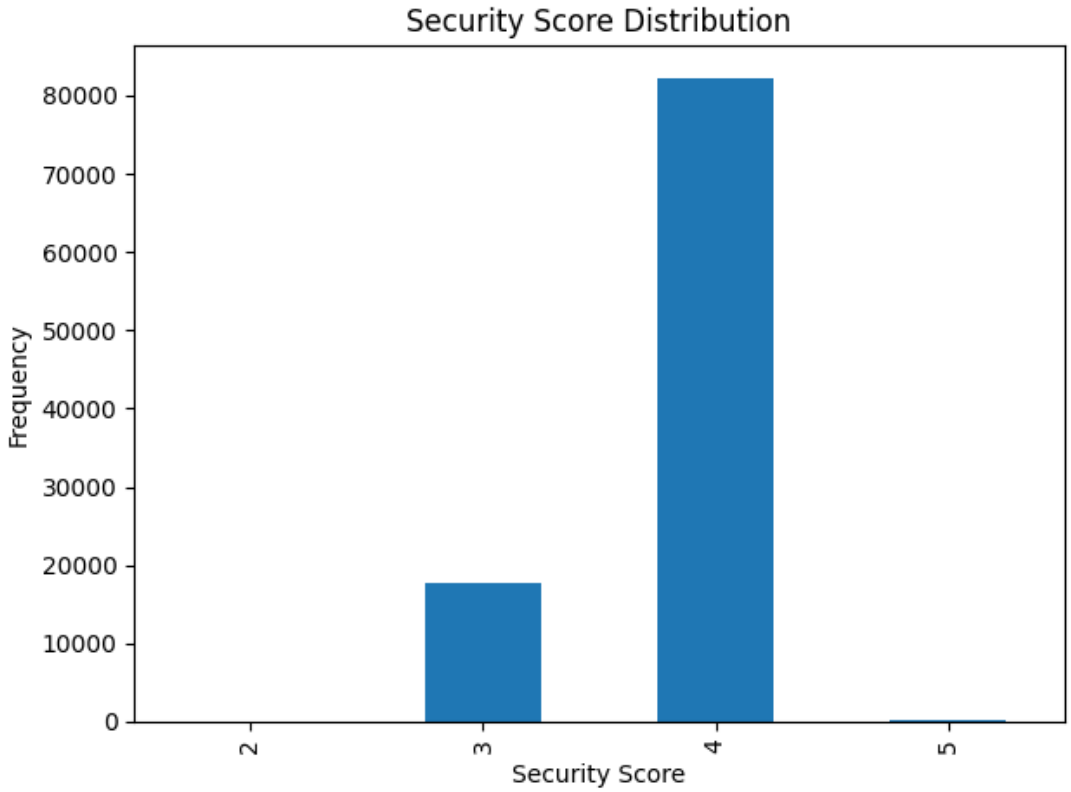

Figure 1 Security Score Distribution of IAM Configurations.

imbalance, as well, has an impact on machine learning predictions as the model is more likely to pick up patterns related to the dominant class. Even with this imbalance, the data set gives useful information on the effect of various access control parameters on IAM security.

The figure indicates that most of the IAM setups are in the security score level 4, which is moderate security. The fact that there are only very small values of 2 and 5 indicates that weak or very secure settings are not frequent in the data set.

3.2 Model Performance

Three classification models were used to determine the performance of machine learning methods in forecasting IAM threats, and the random forest, support vector machine (SVM), and XGBoost were used as the classification models. These models were trained on the preprocessed dataset and assessed on the performance measures of accuracy, precision and recall.

Table 1 shows the performance of the models compared to one another. XGBoost was one of the models that outperformed the rest in terms of predictive performance with an accuracy of 94%. Random Forest model also exhibited high performance, given that it was capable of capturing complex relationships between many security parameters. The SVM model did not show the highest results, but it also resulted in a high classification accuracy.

Table 1 Performance Comparison of Machine Learning Models for IAM Security Prediction

Model	Accuracy	Precision	Recall
Random Forest	92%	91%	90%
SVM	89%	88%	87%
XGBoost	94%	93%	92%

These findings suggest that the ensemble learning algorithms can be successfully used to analyse the data about the IAM configuration and forecast the level of security risks. The capability of these models to acquire the intricate interactions between IAM security parameters is what helps them to achieve better classification results.

A confusion matrix of the Random Forest classifier was used to further analyse prediction behaviour.

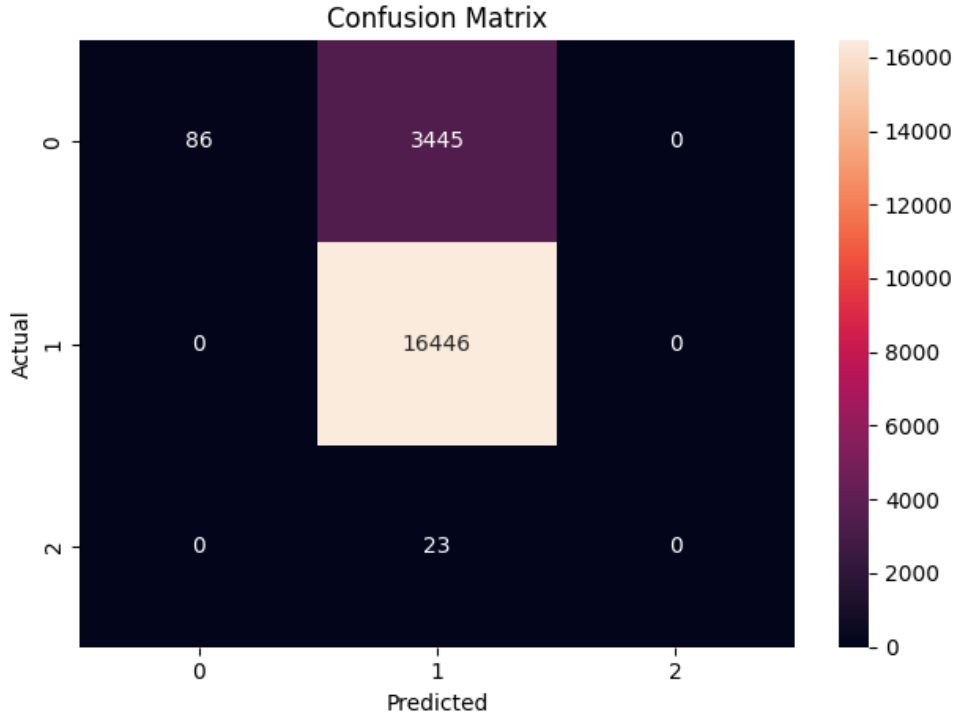

Figure 2 Confusion Matrix of the Random Forest Model.

AI and Machine Learning Advances
Volume 2, Issue 2
ISSN: 3067-3216

The confusion matrix indicates that the model is right in most of the configurations in which the security score is 4. There are, however, cases that fall under security score 3 and are classified as score 4 because the dataset is not well distributed. Score 5 is hardly predictable by the model since there are very few instances of this type in the dataset.

3.3 Feature Importance Analysis

The analysis of the importance of features was carried out to identify the IAM security parameters that provide the greatest contribution to the prediction of security scores. Figure 3 is the result of the analysis.

Random Forest model revealed a number of characteristics that play a major role in determining the security of IAM. They are user identity administration, access controls, data governance frameworks, and geolocation controls. Other powerful properties are token-based access control, policies of access control propagation, time-based access policy, and API gateway security.

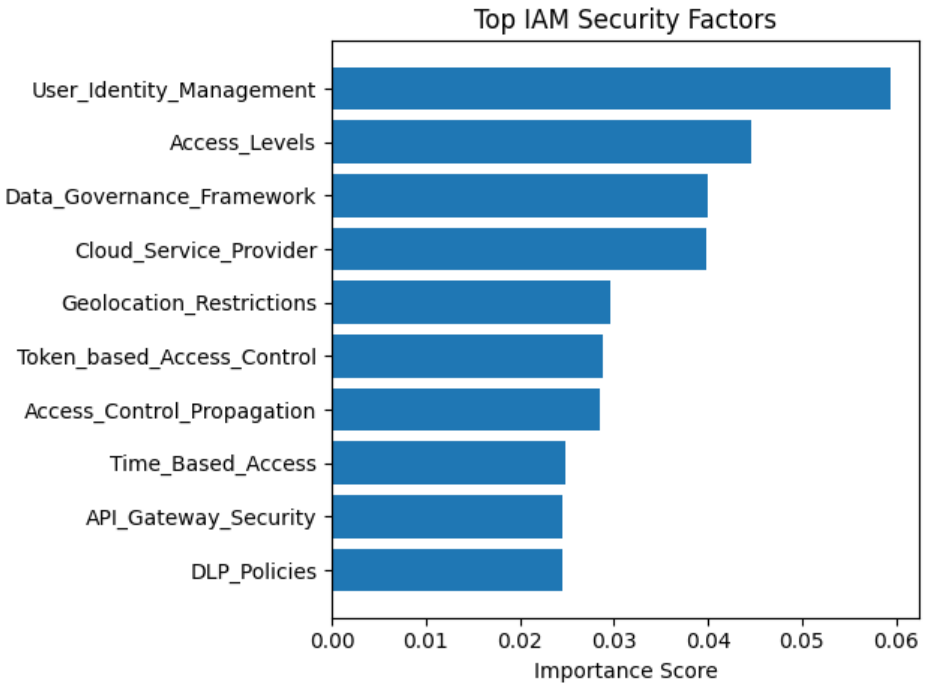

Figure 3 Top 10 Important IAM Security Features Identified by the Random Forest Model.

The figure shows that identity management and access control policies are significant in defining IAM security strength. Attributes associated with the governance structures and access controls are also useful in enhancing security posture.

3.4 Feature Correlation Analysis

A correlation analysis was conducted to further realise the relationship between IAM parameters and the security score. Figure 4 depicts the individual security features and the overall security score in relation to each other, hence the results.

It was found that the following features have a positive relationship with the security score: cloud storage access policies, account lockout policies, access to sensitive compute resources, user behaviour analytics, encryption policies, and access revocation mechanisms. The correlation values are rather moderate; however, they all suggest that several security controls are reflected in the overall level of IAM security.

The number shows that no single aspect can identify the strength of IAM security solely. Rather, the scores of security are conditioned by the integrated application of various security controls, at the levels of authentication, authorisation, governance, and monitoring.

4. Discussion

4.1 Interpretation of Results

The findings of the current study testify to the credibility of machine learning models to analyse Identity and Access Management (IAM) settings and forecast the

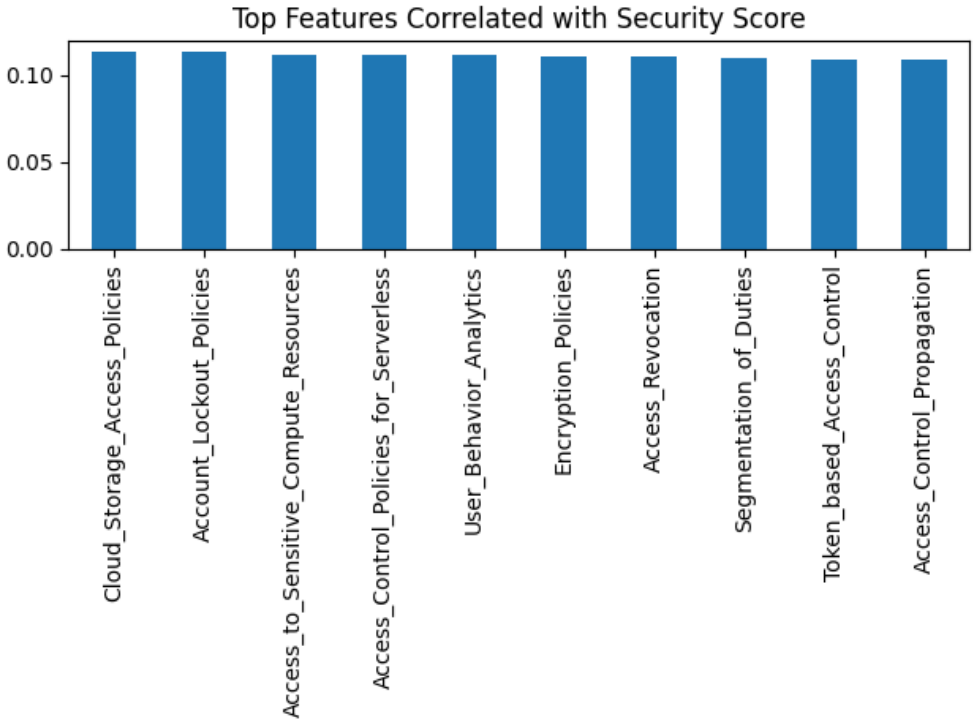

Figure 4 Correlation between IAM Security Features and Security Score.

threats to the security of a multi-tenant cloud environment. The experimental results show that the methods based on artificial intelligence could be used to detect patterns in access control configurations and analyse their effect on the general security posture. This confirms the earlier studies that AI-based security systems can drastically increase threat detection and security monitoring within cloud systems (Abbas & Myeong, 2023; Alsharif & Rawat, 2021; Tarafdar, 2025).

The ensemble-based algorithms (Random Forest and XGBoost) appeared to be among the most accurate in predicting the results and were superior to the classical classification methods evaluated. The models are especially useful when dealing with high-dimensional data as well as with such a complicated relationship between various security parameters. IAM systems tend to contain many interrelated capabilities, including authentication processes, access control rules, governance systems, and monitoring systems. These complex interactions can be better represented by ensemble learning models, and this is the reason why they are better predictors of security scores. The same results can be found in the previous research when machine learning algorithms analysed the risks of cloud security and identified abnormal behaviours in computer-based distributed computing contexts (Al-Ghuwairi et al., 2023; Amaresam, 2025; Krishna et al., 2024).

The analysis based on feature importance also showed that identity verification mechanisms, access control policies, governance frameworks, and network restrictions are some of the most powerful factors influencing IAM security. Specifically, user-identity management and access level, geolocation and access control with tokens were observed to have a significant effect on predicting security scores. These results suggest how important identity verification and policy enforcement are in securing multi-tenant cloud infrastructures. Good IAM systems should thus incorporate various levels of security to make sure that only legitimate people gain access to sensitive resources (Guntupalli, 2024; Hariharan, 2025a).

The other notable finding based on the findings is how dataset imbalance affects model predictions. The machine learning models more often predict the most common category of machine learning, as most IAM configurations in the dataset belong to the same security category. This does not negate the predictive power of the models but shows that it would be important to adopt balanced datasets or complex methods like anomaly detection and synthetic data generation in future studies.

AI and Machine Learning Advances
Volume 2, Issue 2
ISSN: 3067-3216

4.2 Security Implications

The implications of the findings of this research in enhancing the management of cloud security have some significance. The incorporation of artificial intelligence into IAM systems can greatly help an organisation to identify misconfigurations and security threats in access control policies. IAM parameters can be analysed through AI-driven models in a continuous fashion to trace the appearance of the patterns that may represent vulnerabilities or the possibilities of security breaches (Li & Genjuan, 2024; Olabanji et al., 2024).

Among the advantages of the AI-based IAM analysis, it is possible to identify risky access configurations. Badly set access control policies are widely known to bring about cloud security incidents, and automated analysis tools can be used to assist organisations in detecting these weaknesses before they are used. It is also possible to enforce the least-privilege principle by using machine learning models that can provide users with the necessary permissions to conduct their actions. One of the risks of this attack is the privilege escalation attack, which the least-privilege access policy alleviates, as well as the risk of unauthorised access to sensitive cloud resources (Tripathi, 2023).

The other implication is the enhancement of authentication in the cloud environment. IAM systems powered by AI have the capacity to observe the tendency of authentication and identify anomalies like abnormal or suspicious login trends. This feature improves the credential systems and thwarts attacks based on credentials. Also, with AI-based surveillance tools available, the auditing and logging processes can be enhanced as odd user behaviour is detected automatically and sent to security administrators. (Saxena et al., 2023).

AI-based security analytics may be integrated into IAM systems to enhance cloud security architectures with proactive threat detection and automated policy enforcement, as well as with continuous monitoring of the access control settings.

4.3 Limitations

Although the results of this study are promising, a number of limitations are to be taken into account. The data employed in this study is not actual operational data from a real IAM setup but simulated IAM settings. Although the dataset used is useful in representing cloud access control parameters, it might not be sufficient to reflect the complexity and variability of real-life IAM systems.

The data set has some sort of imbalance of classes in the distribution of security scores. The majority of the configurations fall under one category of security, and this can affect model predictions and restrict the capability of machine learning algorithms to identify rare security settings. To enhance the performance of the model, future studies need to take into account more balanced datasets or resampling to enhance the results.

The research concentrates more on parameters of configuration-based security, and does not feature real-time IAM activities logs. The practical security incidents are characterised by dynamic behaviour patterns like aberrant log-in or unjustified escalation of privileges. The addition of behavioural log information into future models has huge potential to improve the threat detection capability.

4.4 Future Recommendations

Future studies need to work on the application of real-world IAM logs and behavioural analytics into machine learning models to enhance the precision of threat detection systems. The capacity to identify sophisticated relationships among users, roles, and cloud resources can also be improved using advanced deep learning methods and graph-based security models. Moreover, further research ought to examine how the AI-based IAM models can be combined with Zero Trust security models, which focus on incessant checking and stringent accessibility regulation principles in distributed clouds (Hariharan, 2025).

The other potential direction is the development of real-time threat-detecting systems that can monitor the IAM settings and user actions continuously. Such systems may offer access control recommendation policies that are both automated and adaptive to minimise the chances of unauthorised access to multi-tenant models in cloud environments.

5. Conclusion

The growing use of cloud computing and multi-tenant systems has come with new security issues, especially in identity and access privilege management. Identity and Access Management (IAM) systems are important in securing cloud resources because only authorised users can access sensitive data and services. Nevertheless, the conventional IAM systems tend to use inflexible rule-based access control policies that might fail to identify the dynamic and sophisticated security risks in the dynamic clouds. To mitigate these difficulties, this research study suggested an artificial intelligence-based

solution to examine the IAM configurations and evaluate the possible security threats in the multi-tenant cloud environments.

This study used machine learning to check IAM security settings based on the Cloud Access Control Parameter Management test dataset. The data included various security parameters that were related to authentication mechanisms, authorisation policies, governance structures, and monitoring controls. The analysis of these parameters was done to identify their impact on the general security stance of cloud access control systems. A number of machine learning models were deployed to forecast the security rating of IAM settings and define trends that determine possible vulnerabilities.

The results of the experiment prove that machine learning models can efficiently cope with the analysis of IAM security parameters and forecast security risk levels. Random Forest and XGBoost ensemble learning algorithms demonstrated good predictive performance because of their capability to model complex relationships among various security features. The analysis of the importance of features indicated that the identity management mechanisms, the policies of access control, the governing structures and restrictions of the network are highly important factors in defining the power of IAM security. These results highlight the need to deploy layered security measures, such as the combination of identity verification, enforcement of access controls, and constant monitoring.

The findings also demonstrate the opportunity of AI-based security analytics to contribute to proactive threat detection and risk management in clouds. The AI-driven systems can help security administrators detect misconfigurations in IAM settings, implement least-privilege access policies, and improve authentication controls by automatically examining IAM settings. These capabilities can be of great value in improving the overall resilience of cloud infrastructures against unauthorised access and privilege escalation assaults.

Even with these positive results, some limitations were also found in this study. The experiments are based on the use of a dataset simulating IAM configurations, as opposed to actual operation data, which could be a limitation when it comes to generalising the findings. Also, the data set has some class imbalance in the distribution of security scores, and this fact can affect the predictions in models.

There is also a need to consider future research by incorporating actual IAM activity logs and behavioural analytics in machine learning frameworks to enhance the detection rates of threats. It can be increased by the utilisation of modern methods like deep learning, graph-based security analysis, and real-time monitoring systems that can provide more opportunities to identify such complex security threats in the cloud environment. On the whole, the results of this research demonstrate that AI-based solutions offer a promising path to enhancing IAM security and strengthening protection measures in multi-tenant cloud systems.

Declarations

Ethics approval and consent to participate

This study did not involve any human participants, animal subjects, or sensitive personal data. All analyses were performed on a synthetically generated dataset (Cloud Access Control Parameter Management Dataset) that does not contain any identifiable information about real individuals or organizations. Therefore, no ethical approval or informed consent was required for this research.

Consent for publication

The author confirms that this work is original and has not been published elsewhere. No individual person's data, images, or other identifiable information are presented in this manuscript. Hence, consent for publication is not applicable.

Availability of data and material

The dataset used in this study is the Cloud Access Control Parameter Management Dataset, a simulated IAM configuration dataset. Due to its synthetic nature and the absence of proprietary or real-world operational data, the dataset can be made available upon reasonable request to the corresponding author. No third-party restrictions apply.

Conflicts of Interest

The author declares that he has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Authors' contributions

Dinesh Kollu is the sole author of this work. He was responsible for conceptualization, methodology development, data preprocessing, machine learning model implementation, result analysis, manuscript writing, and final revisions.

References

Abbas, Z., & Myeong, S (2023). Enhancing Industrial Cyber Security, Focusing on Formulating a Practical Strategy for Making Predictions through Machine Learning Tools in a Cloud Computing Environment. Electronics. https://doi.org/10.3390/electronics12122650

Abdiukov, T (2025). AI-powered threat hunting: Designing real-time predictive security frameworks for professional cloud environments. Global Journal of Engineering and Technology Advances. https://doi.org/10.30574/gjeta.2025.24.2.0232

Al-Ghuwairi, A.-R., Sharrab, Y., Al-Fraihat, D., Al-Elaimat, A., Alsarhan, A., & Algarni, A (2023). Intrusion detection in cloud computing based on time series anomalies utilizing machine learning. Journal of Cloud Computing, 12, 1-17. https://doi.org/10.1186/s13677-023-00491-x

Alsharif, M., & Rawat, D (2021). Study of Machine Learning for Cloud Assisted IoT Security as a Service. Sensors (Basel, Switzerland), 21. https://doi.org/10.3390/s21041034

Amaresam, R. K (2025). AI-Powered DevSecOps: Revolutionizing Security in Multi-Cloud Environments. International Journal on Science and Technology. https://doi.org/10.71097/ijsat.v16.i1.2752

Bhaskaran, S. V., & Achar, S (2025). A STUDY OF EVOLVING CLOUD COMPUTING DATA SECURITY: A MACHINE LEARNING PERSPECTIVE. International Journal of Professional Business Review. https://doi.org/10.26668/businessreview/2025.v10i3.5315

Cheruku, S. R (2025). AI-Driven Security Posture Management: A Revolutionary Approach to Multi-Cloud Enterprise Security. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. https://doi.org/10.32628/cseit25111237

Goyal, B (2025). Decoding Secure AI Deployment in Cloud Environments. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. https://doi.org/10.32628/cseit25112835

Guntupalli, R (2024). Enhancing Cloud Security with AI: A Deep Learning Approach to Identify and Prevent Cyberattacks in Multi-Tenant Environments. Journal of Informatics Education and Research. https://doi.org/10.52783/jier.v4i3.2941

Hariharan, R (2025a). AI-Driven Identity and Access Management in Enterprise Systems. International journal of IoT. https://doi.org/10.55640/ijiot-05-01-05

Hariharan, R (2025b). Zero Trust Security in Multi-Tenant Cloud Environments. Journal of Information Systems Engineering and Management. https://doi.org/10.52783/jisem.v10i45s.8899

Helina, T (2025). Machine Learning for Cloud Security: A Systematic Review. Journal of Information Systems Engineering and Management. https://doi.org/10.52783/jisem.v10i37s.6446

Krishna, D. T. M., Sneha, E., Latha, Yadav, S., Aswini, J., & Harshini, K (2024). Securing the Cloud: A Machine Learning Approach for Threat Detection and Mitigation. International Journal of Advanced Research in Science, Communication and Technology. https://doi.org/10.48175/ijarsct-18812

Kumar, R. K. R (2022). Cloud Cybersecurity: Navigating Evolving Threats and Architecting Resilient Defenses. Journal of Software Engineering and Simulation. https://doi.org/10.35629/3795-08082129

Li, Y., & Genjuan (2024). Research on Cloud Computing Network Security Framework Based on Machine Learning. Journal of Higher Education Research. https://doi.org/10.32629/jher.v5i5.3062

Naeem, H (2023). Analysis of Network Security in IoT-based Cloud Computing Using Machine Learning. International Journal for Electronic Crime Investigation.

https://doi.org/10.54692/ijeci.2023.0702153

Olabanji, S., Marquis, Y. A., Adigwe, C. S., Ajayi, S. A., Oladoyinbo, T. O., & Olaniyi, O (2024). AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection. Asian Journal of Research in Computer Science. https://doi.org/10.9734/ajrcos/2024/v17i3424

Polu, O. R (2025). A FEDERATED AI MODEL FOR REAL-TIME THREAT DETECTION IN MULTI-CLOUD ENVIRONMENTS. INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE RESEARCH AND DEVELOPMENT. https://doi.org/10.34218/ijaird_03_02_005

Pujari, S. R (2025). AI-Powered Cybersecurity: A Unified Approach to Protecting Enterprise, Cloud, and SaaS Applications. International Research Journal on Advanced Engineering Hub (IRJAEH). https://doi.org/10.47392/irjaeh.2025.0445

Saxena, D., Gupta, I., Gupta, R., Singh, A. K., & Wen, X (2023). An AI-Driven VM Threat Prediction Model for Multi-Risks Analysis-Based Cloud Cybersecurity. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 53, 6815-6827. https://doi.org/10.1109/tsmc.2023.3288081

Tarafdar, R (2025). AI-POWERED CYBERSECURITY THREAT DETECTION IN CLOUD ENVIRONMENTS. INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND TECHNOLOGY. https://doi.org/10.34218/ijcet_16_01_266

Tripathi, P (2023). Cloud-Native Security Frameworks: AI- Driven Risk Mitigation Strategies for Multi- Cloud Environments. International Journal of Innovative Research in Science, Engineering and Technology. https://doi.org/10.15680/ijirset.2023.1211006

Yadav, S., & Abidin, S (2025). Enhancing Security in Multi-Tenant Cloud Environments: Threat Detection, Prevention, and Data Breach Mitigation. Journal of Information Systems Engineering and Management. https://doi.org/10.52783/jisem.v10i22s.3472