International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 1 (2026)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 1, 2026

Peer Reviewed, Referred & Indexed Journal

Paper Research

ENHANCING CLOUD SECURITY: EMPOWERING MACHINE LEARNING TO COMBAT PRIVILEGE ESCALATION ATTACKS

[1] Nazeemullah Hayatullah, [2] Dr. K. Santhi Sree

[1] MCA Student, Department of Information Technology, Jawaharlal Nehru Technological University Hyderabad, Telangana, India

[2] Professor, Department of Information Technology, Jawaharlal Nehru Technological University Hyderabad, Telangana, India

Abstract: This project is based on machine learning to ensure cloud security is made more resilient by targeting and preventing privilege escalation attacks. The probability of the attack of privilege escalation increases with the increased population of cloud users. The project seals gaps in the access control of employees to the services offered by the clouds in order to make the entire system more secure. In the project, machine learning is used to detect and prevent privilege escalation attacks in real time. Some of the tools include LightGBM, Random Forest, Adaboost and Xgboost which can assist in maintaining your defences against emerging threats. The users and organisations are assured of the safety of their data thus creating confidence upon cloud computing. The security improvements by the project will make cloud service providers and businesses feel more secure as they are online. The system can better detect and prevent attempts of privilege escalation with the help of a Voting Classifier, which integrates predictions by the Decision Tree, Random Forest and Support Vector Machine using a soft voting strategy. Moreover, user testing can be simplified with the help of a user-friendly Flask application with SQLite integration that also includes secure signup and signin functions that can be tested and used in the real life.

Index Terms *- Privilege escalation, insider attack, machine learning, random forest, adaboost, XGBoost, LightGBM, classification.*

Received: 08-12-2025 Accepted: 21-01-2026 Published: 28-01-2026

I. INTRODUCTION

Cloud computing is a novel way of thinking about how to simplify the process of people using the Internet and access services. The current in place infrastructure. Cloud storage providers do minimal actions in order to secure their systems and data they store them, including encryption, access control, and authentication. All types of data of various forms can be stored in the cloud at any time, and it is feasible, provided it is easy to access, fast and frequent. Businesses and cloud service providers are passing a lot of data between each other, either intentionally or accidentally, which may cause sensitive information breaches. Ease of using internet services by workers and IT systems is what makes the task of firms preventing people to get in hard [2]. Cloud services create more security risks to businesses, including authentication and open interfaces. Advanced hackers employ their knowledge to intrude into Cloud systems. There are many algorithms and methods employed by machine learning to enhance the management of data and to address security problems. A lot of datasets are confidential, and cannot be shared due to the privacy considerations, or they might lack significant statistical properties [3], [4].

The Cloud market is becoming rapidly expanding, and this aspect makes the concern of privacy and security to be regulated by regulations. Access rights might not change when an employee finds new responsibilities

and positions within the Cloud Company. Due to this, there is exploitation of old privileges, which are not beneficial to steal and destroy valuable data. Each of the accounts speaking to a computer is powerful to some extent. The unapproved people are not able to access the server databases, private files, and other services. An attacker can obtain access to a sensitive system by completing an overthrow of a higher-level user account and by utilizing the privileges or extending the privileges of that account. Attackers may move horizontally to have control over additional systems or vertically to gain access to the administrator and root privileges until they are in full control of the entire environment [1]. Horizontal privilege escalation occurs when a user obtains the access privilege of another user with similar access level. The horizontal privilege escalation allows an attacker to access information that is not related to him. A hacker may identify the vulnerabilities in a poorly developed web program that would enable him access information of other people [3], [5]. Since the attacker has completed a horizontal elevation of privileges exploit, he/she can view, alter, and duplicate confidential data.

Attackers target data sources due to the privacy and the most important information. In case of the loss of data, it will impact the privacy and security of all cloud users. Those who do ill things, but have permission are referred to as an insider threat. Due to the rapidly increasing rate of networks, many businesses and groups have established their own internal networks. According to recent estimates 90 percent of firms believe that they may be attacked within [7]. Privilege elevation enables the attackers to discover additional methods of attacking a target system. Trying to escalate privileges, insider attackers are interested in gaining further access to sensitive systems or more privileges. Insider attacks are difficult to identify and prevent because they occur under the security measures of the company and in most cases they are granted to access the network. Locating and classifying insider risks has now been difficult and tedious [8].

Recent researches have been involved in detecting and classifying privilege escalation attacks by the individuals who are insiders. They proposed different machine learning and deep learning algorithms to solve these challenges. Other recent research used SVM, Naive Bayes, CNN, Linear Regression, PCA, random Forest, and KNN. However, due to the abundance of various types of attacks, there is an enormous need in rapid and efficient machine learning algorithms. We must, therefore, have an efficient and expeditious method of detecting, categorizing, and preventing these insider attacks. This is why we must have smart algorithms, such as ML algorithms, that would sort and predict insider threats to improve security systems.

Furthermore, the understanding of the performance of the ML algorithms in detecting insider assaults allows you to select the most suitable algorithm in each case in question, and the algorithms (ML algorithms) should be enhanced. So you can keep things safer. This project will aim at utilizing effective and efficient ML algorithms on insider assault instances to achieve improved and faster results. The following ML algorithms have been used and tested by us: Random Forest, AdaBoost, XGBoost, and LightGBM. The boosting technique is based on the idea that a bad classifier can be made much better through boosting the prediction of the classification algorithm. Random Forest, AdaBoost, and XGBoost performed very well in terms of their rapid and accurate insider threat classification.

II. LITERATURE REVIEW

Cloud computing can be described as the capability to acquire PC framework resources on demand. Particularly, the possibility of storing and handling information but not having the client to directly control it. It has provided individuals with the power of having the public and private computing and data storage on a single platform via the Internet. It also contains several security issues and

threats that might restrain the application of the cloud computing technologies. [5]. In this paper, the discussion is on the risks, issues, approaches and solutions to cloud computing security. In a previous survey, a significant number of the participants expressed concern regarding security. The other survey examines the model of cloud computing architecture and some of them discuss about security concerns and the methods of managing them. This article brings all the concerns, issues, strategies, and solutions related to security together.

Cloud computing refers to the ability to use on-demand resources of personal computer systems such as storage space and computing power without the input of the client. Email is frequently used to share and obtain data by people and groups. Individuals are routinely transferring confidential data such as credit reports and financial data on the Internet. [1]. Phishing is one of the means that criminals use to rob sensitive information off people posing as trusted entities. A spoomed email will fool you to provide the sender with confidential details. This is simply because individuals are receiving and sending phishing emails. The attacker subjects you to junk email, and when you open and read the email, they receive your information. Everyone has been concerned with it during the past few years. The research uses different valid and phishing datasets, recognises new emails, and uses different attributes and algorithms in the process of categorisation. A new dataset is created after consideration of the existing approaches. We created a created feature comma-separated values (csv) file, and a label file. Then we employed the support vector machine (SVM) [8, 10], Naive Bayes (NB), and long short-term memory (LSTM) approach [1, 27]. The identification of a phished email is handled in this experiment as a classification problem. The comparison and implementation indicate that SVM, NB, and LSTM are more superior and precise in detecting phishing emails. All the three classifiers (SVM, NB, and LSTM) were doing very well in classifying email attacks with an accuracy of 99.62, 97, and 98 respectively.

Cloud computing is the novelty of the market as science and technology are improving. One way that helps to secure data is through cloud cryptography [4]. The primary advantage of the use of cloud storage is that it is simple to access, does not demand a significant amount of equipment, is affordable to secure, and is simple to replace hence all businesses use it. Encryption refers to the act of coded information in order to be able to be viewed by individuals who are supposed to. Today we want to safeguard the information we archive in our computers or forward it through the internet against attacks. [4]. The cryptography model is grounded on their response speed, their privacy, their bandwidth, and their reliability. Security is also one of the largest portions of cloud computing that ensures the safety of client data stored in the clouds. The article under our study examines the effectiveness of various cryptographic algorithms, the frequency of their application, and their utility. Evaluation findings reveal what approach is most appropriate to use in the context of what type of data.

Due to the high number of people who are using technology these days, numerous security issues have been raised. The general population as well as the business world spends a considerable amount of money in ensuring that their information remains secure against attacks that may jeopardize its privacy, integrity and availability. One of the forms of attack which are more horrible than external attacks is the insider attacks. The reason behind this is that, insiders are authorised people who have actual access to sensitive assets of an organization [36]. Therefore, the literature is full of studies aimed to develop methods and tools that could be used to detect and prevent various types of insider risks. This paper will analyse some of the strategies and defences proposed to prevent insider attacks. It proposes one unified classification methodology that divides insider threat prevention strategies into two: biometric

based, and asset based metrics. [36, 37] The biometric-based is further subdivided into physiological, behavioural, and physical classifications whereas the asset metric-based classification is further divided into host, network, and combination classifications. This categorises the reviewed methodologies which are empirically supported using the grounded theory approach to ensure a comprehensive literature review. The article also compares and discusses significant theoretical and empirical considerations that are critical when making insider threat prevention techniques effective (e.g., datasets, feature domains, classification algorithms, evaluation metrics, real-world simulation, stability and scalability, etc.). It also discusses some of the large issues which should be considered when implementing practical solutions to prevent insider threats. It also has certain research gaps and recommendations on future study directions.

One of the technologies that are rapidly evolving is the Internet of Things [34]. It links computers and sensors together to enable them exchange data through the network to determine various issues and provide new services. IoT is a significant technology that enables smart houses. The smart home technology also provides customers with many convenient options, like the opportunity to check the temperature, detect smoke, automatically control lights, and use smart locks. However, there are also new security and privacy issues, which emerge due to technology. As an example, one may gain access to confidential user information by gaining control of the surveillance cameras or even triggering false fire alarms. Such issues make smart homes vulnerable to various types of security attacks, and the consumers are unwilling to adopt this technology due to issues with security. In this survey paper [6], we illuminate the Internet of things (IoT), the IoT development, the objects and their specifications, the layered architecture of the IoT setting, and the numerous security issues that emerge in every level within the smart house. This paper explains the issues and challenges that arise in smart homes utilizing the Internet of Things (IoT), and provides different concepts that can address the security concerns.

III. METHODOLOGY

The proposed solution is a machine learning-powered method of locating and categorizing insider threats on clouds. The predictions are more accurate with the use of the Random Forest, Adaboost, XGBoost, and LightGBM algorithms. To make the proposed system more accurate in detecting insider threats, a number of machine learning algorithms, including Random Forest, Adaboost, XGBoost [35], and LightGBM, are used. The system applies ensemble learning methods to combine the finest aspects of numerous systems, and this enhances the general capacity of forecasting insider threats in the clouds. Data preparation techniques, such as data aggregation and normalisation, which are very powerful, are used in this system to address such issues as the absence of values, outliers, and features not valuable to the model performance improvement. Parameters such as learning rate, maximum depth and K-fold are adjusted in order to make the machine learning models to work. This renders the detection of insider threats more efficient and specific to every case. And it also contained a Voting Classifier that was comprised of the predictions of Decision Tree, Random Forest, and Support Vector Machine [10] using a soft method of voting. This improved the system of detecting and preventing privilege escalation attacks. The ease of user testing is further facilitated by a user-friendly Flask structure with SQLite as part of it that enables users to signup and signin, which is convenient to the real-world use and test.

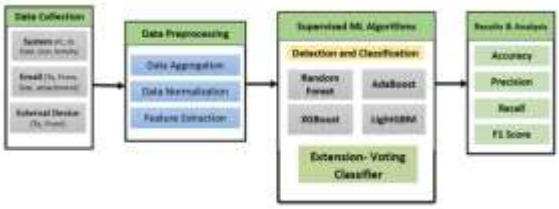


Fig 1 Proposed architecture

The system architecture has four primary sections: data gathering, data cleanup, application of supervised machine learning algorithms and the analysis of findings. In data collection stage, a customized set of data available in different files of the CERT dataset is used. Subsequently, the obtained data undergoes preprocessing which involves such process as aggregation of the data, normalisation and obtaining of features to make it more acceptable and feasible. The core of the system consists of the application of machine learning algorithms such as Random Forest, AdaBoost, XGBoost, and LightGBM [31, 32] and a voting classifier as an extension in order to identify and rank the threats of privilege escalation in the processed data. Finally, the system makes an in depth analysis of the results, which includes how individual algorithms perform and provides information on the performance of the entire system on detection of insider threats. This architecture ensures a systematic and robust approach of countering the privilege escalation attacks through machine learning processes.

A) Dataset collection:

This study relies upon the data provided by a number of files in the CERT dataset [13, 14], but concerns the information that is connected with emails. This is a well-selected data set comprising some examples that are applicable to insider threat scenarios during email communications. It contains many various features, characteristics, which are related to the behavior of the users, to what they write in their emails, and the way they treat the system.

Fig 2 CERT dataset

B) Data Processing:

When analysing data, you transform raw data into viable data on businesses. Data scientists typically handle information through collection, sorting, cleaning, verification, analysis and transforming it to graphs or documents that can be read by humans. Data can be processed using three methods, including death by hand, machine, or computer. The aim is to render information more practical and assist individuals in making decisions. This assists the companies to manage their businesses more efficiently and make crucial decisions in time. This is a large part of the automated data processing tools such as computer programming. It is capable of putting into perspective a large amount of data and especially big data to enable you to make superior judgments and manage quality.

C) Feature selection:

The process of selecting the most useful, consistent and non-redundant features to use when constructing a model is referred to as feature selection. Due to the continuous increase in the volume and size of datasets, it is critical to reduce them systematically. The general idea of feature selection is to ensure a predictive model is more effective and will be less expensive to execute.

A large portion of feature engineering involves feature selection. It is the mechanism of making the most significant features to feed the machine learning algorithms. To reduce the number of input variables, the input variables are reduced by filtering them with feature selection strategies that eliminate unnecessary variables or those that are too tightly correlated with other variables. This reduces the number of features to the most significant ones to the machine learning model. The main advantages of feature selection predefining rather than having the machine learning model select which features are the most important.

D) Algorithms:

LightGBM: It is a gradient boosting ensemble that utilizes decision trees. It is used in the Train Using AutoML application. Similar to other methods based on the decision trees, LightGBM can be employed in classification and regression. LightGBM can be configured to be used in distributed systems [31, 32].

$$F_m(x) = F_{m-1}(x) + \eta \cdot h_m(x)$$

XGBoost: How XGBoost Works - Amazon SageMaker XGBoost is a popular and efficient open-source implementation of the gradient boosted trees algorithm. Gradient boosting is a supervised learning algorithm, which attempts to accurately predict a target variable by combining the estimates of a set of simpler, weaker models [35].

$$y\hat{}_i = \sum_{k=1}^{K} f_k(x_i), f_k \in F$$

AdaBoost: Adaptive Boosting is also called AdaBoost and it is a Machine Learning algorithm that can be described as an Ensemble Method. The commonest kind of estimator that is employed with AdaBoost is a one-level decision tree or in other words, a decision tree that is split only once. These trees are also known as decision stumps.

$$F(x) = \sum_{t=1}^{T} \alpha_t h_t(x)$$

RF: Random forest is a trademark by Leo Breiman and Adele Cutler. Random forest is an effective machine learning algorithm that uses the results of hundreds of decision trees to come up with a single answer. The reason why it is popular is that it is simple to apply and flexible, and resolves both classification and regression [34].

$$y\hat{} = \arg\max_k \sum_{t=1}^{T} 1(h_t(x) = k)$$

VC: A Voting Classifier is a form of machine learning model that learns by example of a collection of other models and predicts a single class (vehicles) by taking into consideration the class that is most likely to be selected as the output.

$$y\hat{} = \arg \max_c \sum_{i=1}^{N} w_i 1(hi(x) = c)$$

IV. EXPERIMENTAL RESULTS

Accuracy: The accuracy of a test is its ability to differentiate the patient and healthy cases correctly. To estimate the accuracy of a test, we should calculate the proportion of true positive and true negative in all evaluated cases. Mathematically, this can be stated as:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} (1)$$

Precision: Precision evaluates the fraction of correctly classified instances or samples among the ones classified as positives. Thus, the formula to calculate the precision is given by:

$$Precision = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}} (2)$$

Recall: Recall is a metric in machine learning that measures the ability of a model to identify all relevant instances of a particular class. It is the ratio of correctly predicted positive observations to the total actual positives, providing insights into a model's completeness in capturing instances of a given class.

$$Recall = \frac{TP}{TP + FN} (3)$$

F1-Score: F1 score is a machine learning evaluation metric that measures a model's accuracy. It combines the precision and recall scores of a model. The accuracy metric computes how many times a model made a correct prediction across the entire dataset.

$$F1\ Score = 2 * \frac{Recall\ X\ Precision}{Recall + Precision} * 100(1)$$

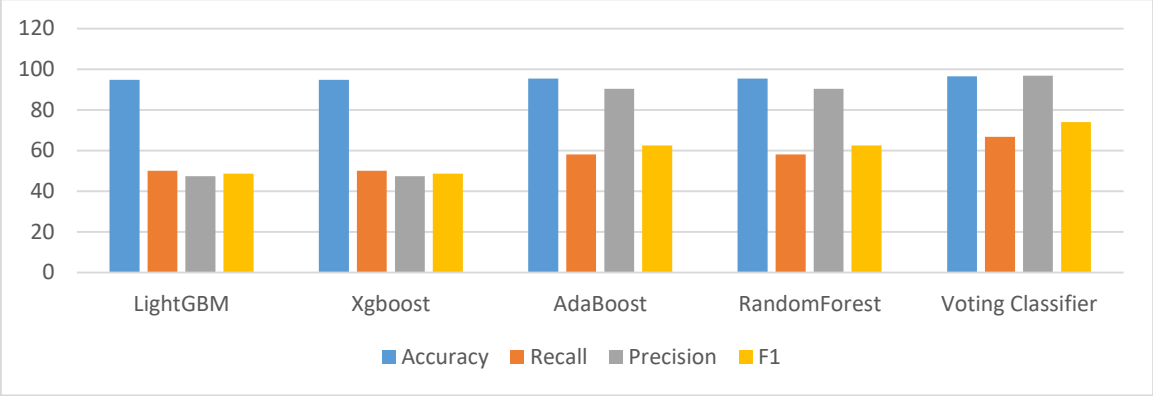
Table(1) evaluate the performance metrics—accuracy, precision, recall and F1-Score—for each algorithm. Across all metrics, the Voting Classifier consistently outperforms all other algorithms. The tables also offer a comparative analysis of the metrics for the other algorithms.

Table.1 Performance Evaluation Metrics for Extra Tree FS

Model	Accuracy	Recall	Precision	F1
LightGBM	94.75	50	47.375	48.65212
Xgboost	94.75	50	47.375	48.65212
AdaBoost	95.45	58.01608	90.27778	62.42581

RandomForest	95.45	58.01608	90.27778	62.42581
Voting Classifier	**96.45**	**66.64028**	**96.82903**	**73.90277**

Graph.1 Comparison Graphs



In Graphs (1), the bright blue and orange represent the accuracy and recall, respectively, the grey and light yellow indicate the precision and the F1-Score, respectively. The Voting Classifier performs better in all measures having the highest scores. These findings are presented in a graphic manner as indicated by the graphs above.

V. CONCLUSION

The evil inside agent is a significant risk to the organisation since he or she has greater access and opportunities to do a lot of harm. The insiders are the ones who have access to privileged and proper information and resources that outsiders do not have. The proposed research involved the application of machine learning to detect and categorize an insider attack. [14]. A customised dataset used in this work is comprised of data in a number of files in the CERT dataset. On that dataset, four machine learning techniques were applied and performed better. These algorithms are the Random Forest, AdaBoost, XGBoost and LightGBM. The results presented in this article were successful experiments that employed the use of supervised machine learning methods, which have more significant accuracy in the classification report. LightGBM is the most accurate algorithm with 97 percent. Accuracies of the other algorithms are 86% in RF, 88% in AdaBoost and 88.27% in XGBoost [31, 32]. The proposed models can be further enhanced in the future by increasing the size and diversity of the dataset regarding its features and the emerging trends of insider attackers to carry out the attack. This may result in novel lines of investigation in the identification and categorization of insider attacks in different sections of business. Businesses employ machine learning models in making plausible business choices and the better the model performance, the better the choices. Errors are rather costly, yet improving the model will reduce the cost. In machine learning (ML)-driven research, users may provide the computer algorithms with large volumes of data, which they further use to make decisions, suggestions and assessments.

VI. FUTURE SCOPE

The further development should be aimed at making the system more scalable to be capable of handling larger workloads in a large configuration of the cloud without being slowed down, even as the scale of data and its intricacy increases. The next step should be the implementation of the dynamic reaction systems, which will be able to locate and eliminate new tactics that are employed in the privilege escalation attacks within a short period of time. This will give a proactive protection against insider threats that are dynamic in nature. It should be remembered to mix techniques whereby decisions made in the models are easier to describe. This transparency can make security analysts have confidence in the outcomes of the system as it

allows them to comprehend what influences the identifications of the threats [29, 30]. The system should also be established to constantly refresh and update the dataset necessary to train the models. Continuous enrichment ensures that the system can continue to locate and prevent emerging types of attacks as well as evolving patterns of insider threats.

REFERENCES

[1] U. A. Butt, R. Amin, H. Aldabbas, S. Mohan, B. Alouffi, and A. Ahmadian, ‘‘Cloud-based email phishing attack using machine and deep learning algorithm,’’ Complex Intell. Syst., pp. 1–28, Jun. 2022.

[2] D. C. Le and A. N. Zincir-Heywood, ‘‘Machine learning based insider threat modelling and detection,’’ in Proc. IFIP/IEEE Symp. Integr. Netw. Service Manag. (IM), Apr. 2019, pp. 1–6.

[3] P. Oberoi, ‘‘Survey of various security attacks in clouds based environments,’’ Int. J. Adv. Res. Comput. Sci., vol. 8, no. 9, pp. 405–410, Sep. 2017.

[4] A. Ajmal, S. Ibrar, and R. Amin, ‘‘Cloud computing platform: Performance analysis of prominent cryptographic algorithms,’’ Concurrency Comput., Pract. Exper., vol. 34, no. 15, p. e6938, Jul. 2022.

[5] U. A. Butt, R. Amin, M. Mehmood, H. Aldabbas, M. T. Alharbi, and N. Albaqami, ‘‘Cloud security threats and solutions: A survey,’’ Wireless Pers. Commun., vol. 128, no. 1, pp. 387–413, Jan. 2023.

[6] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal, ‘‘Smart home security: Challenges, issues and solutions at different IoT layers,’’ J. Supercomput., vol. 77, no. 12, pp. 14053–14089, Dec. 2021.

[7] S. Zou, H. Sun, G. Xu, and R. Quan, ‘‘Ensemble strategy for insider threat detection from user activity logs,’’ Comput., Mater. Continua, vol. 65, no. 2, pp. 1321–1334, 2020.

[8] Reddy, S. K. R. Tailoring Loyalty Rewards Systems across Industries: Cloud vs On-Prem Solutions. International Journal of All Research Education and Scientific Methods (IJARESM),April 2025, ISSN: 2455-6211.

[9] D. C. Le, N. Zincir-Heywood, and M. I. Heywood, ‘‘Analyzing data granularity levels for insider threat detection using machine learning,’’ IEEE Trans. Netw. Service Manag., vol. 17, no. 1, pp. 30–44, Mar. 2020.

[10] F. Janjua, A. Masood, H. Abbas, and I. Rashid, ‘‘Handling insider threat through supervised machine learning techniques,’’ Proc. Comput. Sci., vol. 177, pp. 64–71, Jan. 2020.

[11] R. Kumar, K. Sethi, N. Prajapati, R. R. Rout, and P. Bera, ‘‘Machine learning based malware detection in cloud environment using clustering approach,’’ in Proc. 11th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT), Jul. 2020, pp. 1–7.

[12] D. Tripathy, R. Gohil, and T. Halabi, ‘‘Detecting SQL injection attacks in cloud SaaS using machine learning,’’ in Proc. IEEE 6th Int. Conf. Big Data Secur. Cloud (BigDataSecurity), Int. Conf. High Perform. Smart Comput., (HPSC), IEEE Int. Conf. Intell. Data Secur. (IDS), May 2020, pp. 145–150.

[13] M. V. Sruthi, "Enhancing the Security of the Internet of Things by the Application of Robust Cryptographic Algorithms," 2025 2nd International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), Bangalore, India, 2025, pp. 1-5, doi: 10.1109/ICCAMS65118.2025.11234102.

[14] J. Kim, M. Park, H. Kim, S. Cho, and P. Kang, ‘‘Insider threat detection based on user behavior modeling and anomaly detection algorithms,’’ Appl. Sci., vol. 9, no. 19, p. 4018, Sep. 2019.

[15] Reddy, S. K. (2025). Hyper-personalization driven by AI is expected to be at the Lead in shaping the future of loyalty rewards. Journal of Emerging Technologies and Innovative Research.

[16] P. Chattopadhyay, L. Wang, and Y.-P. Tan, ‘‘Scenario-based insider threat detection from cyber activities,’’ IEEE Trans. Computat. Social Syst., vol. 5, no. 3, pp. 660–675, Sep. 2018.

[17] Nandigama, N. C. (2025). Enterprise-Grade Aml Threat Detection Using Time Frequency Signals And Spring Boot Microservices. Journal of Computational Analysis and Applications, 26(02). https://doi.org/10.48047/jocaaa.2019.26.02.01.

[18] M. I. Tariq, N. A. Memon, S. Ahmed, S. Tayyaba, M. T. Mushtaq, N. A. Mian, M. Imran, and M. W. Ashraf, ‘‘A review of deep learning security and privacy defensive techniques,’’ Mobile Inf. Syst., vol. 2020, pp. 1–18, Apr. 2020.

[19] D. S. Berman, A. L. Buczak, J. S. Chavis, and C. L. Corbett, ‘‘A survey of deep learning methods for cyber security,’’ Information, vol. 10, no. 4, p. 122, 2019.

[20] N. T. Van and T. N. Thinh, ‘‘An anomaly-based network intrusion detection system using deep learning,’’ in Proc. Int. Conf. Syst. Sci. Eng. (ICSSE), 2017, pp. 210–214.

[21] G. Pang, C. Shen, L. Cao, and A. V. D. Hengel, ‘‘Deep learning for anomaly detection: A review,’’ ACM Comput. Surv., vol. 54, no. 2, pp. 1–38, Mar. 2021.

[22] R. A. Alsowail and T. Al-Shehari, ‘‘Techniques and countermeasures for preventing insider threats,’’ PeerJ Comput. Sci., vol. 8, p. e938, Apr. 2022.

[23] Nandigama, N. C. (2025). Leveraging Chatgpt for Multi-Language Data Engineering Code Generation in Distributed Analytics Systems. Journal of Informatics Education and Research.

[24] M. Abdelsalam, R. Krishnan, Y. Huang, and R. Sandhu, ‘‘Malware detection in cloud infrastructures using convolutional neural networks,’’ in Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD), Jul. 2018, pp. 162–169.

[25] F. Jaafar, G. Nicolescu, and C. Richard, ‘‘A systematic approach for privilege escalation prevention,’’ in Proc. IEEE Int. Conf. Softw. Quality, Rel. Secur. Companion (QRS-C), Aug. 2016, pp. 101–108.

[26] Henry P Cyril. (2025). AI-Driven Self-Healing and Transaction Queuing During Network Outages or Degradation: Architectures, Resilience Models, and Future Directions. International Journal of Advanced Research in Science Communication and Technology, 113. https://doi.org/10.48175/ijarsct-30515.

[27] F. Yuan, Y. Cao, Y. Shang, Y. Liu, J. Tan, and B. Fang, ‘‘Insider threat detection with deep neural network,’’ in Proc. Int. Conf. Comput. Sci. Wuxi, China: Springer, 2018, pp. 43–54.

[28] I. A. Mohammed, ‘‘Cloud identity and access management—A model proposal,’’ Int. J. Innov. Eng. Res. Technol., vol. 6, no. 10, pp. 1–8, 2019.

[29] F. M. Okikiola, A. M. Mustapha, A. F. Akinsola, and M. A. Sokunbi, ‘‘A new framework for detecting insider attacks in cloud-based e-health care system,’’ in Proc. Int. Conf. Math., Comput. Eng. Comput. Sci. (ICMCECS), Mar. 2020, pp. 1–6.

[30] G. Li, S. X. Wu, S. Zhang, and Q. Li, ‘‘Neural networks-aided insider attack detection for the average consensus algorithm,’’ IEEE Access, vol. 8, pp. 51871–51883, 2020.

[31] A. R. Wani, Q. P. Rana, U. Saxena, and N. Pandey, ‘‘Analysis and detection of DDoS attacks on cloud computing environment using machine learning techniques,’’ in Proc. Amity Int. Conf. Artif. Intell. (AICAI), Feb. 2019, pp. 870–875.

[32] N. M. Sheykhkanloo and A. Hall, ‘‘Insider threat detection using supervised machine learning algorithms on an extremely imbalanced dataset,’’ Int. J. Cyber Warfare Terrorism, vol. 10, no. 2, pp. 1–26, Apr. 2020.

[33] M. Idhammad, K. Afdel, and M. Belouch, ‘‘Distributed intrusion detection system for cloud environments based on data mining techniques,’’ Proc. Comput. Sci., vol. 127, pp. 35–41, Jan. 2018.

[34] Shiva Kumara. (2025). Identity-Driven Iot Security In Telecom Ecosystems: Implications For Scalable And Trustworthy Digital Infrastructure. International Journal of Applied Mathematics, 38(12s), 2797–2816. https://doi.org/10.12732/ijam.v38i12s.1588.

[35] J. L. Leevy, J. Hancock, R. Zuech, and T. M. Khoshgoftaar, ‘‘Detecting cybersecurity attacks using different network features with LightGBM and XGBoost learners,’’ in Proc. IEEE 2nd Int. Conf. Cognit. Mach. Intell. (CogMI), Oct. 2020, pp. 190–197.

[36] R. A. Alsowail and T. Al-Shehari, ‘‘Techniques and countermeasures for preventing insider threats,’’ PeerJ Comput. Sci., vol. 8, p. e938, Apr. 2022.

[37] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, ‘‘A systematic literature review on cloud computing security: Threats and mitigation strategies,’’ IEEE Access, vol. 9, pp. 57792–57807, 2021.