RESEARCH PAPER

Machine Learning -Based Detection and Mitigation of Privilege Escalation Attacks in Cloud Systems

S. Krishna Reddy[1*], **Vadla Madhavi**[1]

[1]Department of Computer Science and Engineering, Sree Dattha Institute of Engineering and Science, Sheriguda, Hyderabad, Telangana, India

[1]Assistant Professor (S. Krishna Reddy) | Email: krishnareddy.seelam99@gmail.com

[1]PG Student (Vadla Madhavi) | Email: vadlamadhavi000@gmail.com

***Corresponding Author:** S. Krishna Reddy, Assistant Professor, Department of Computer Science and Engineering, Sree Dattha Institute of Engineering and Science, Sheriguda, Hyderabad, Telangana, India | Email: krishnareddy.seelam99@gmail.com

Abstract— This project applies machine learning to improve cloud security, namely, preventing, and helping to prevent privilege escalation attacks to have a more robust defense mechanism. As the number of cloud adopters increases, the probability of attacks associated with privilege escalation also increases. This project aims at sealing employee access privileges holes in cloud services with an aim of enhancing general security. The project applies machine learning to enable running time detection and prevention of privilege escalation attacks. Such algorithms as as LightGBM, Random Forest, Adaboost, and Xgboost offer a great defense against new threats. People and businesses are enjoying a better level of data security, which is breeding trust in cloud computing. The cloud service providers and companies are assured safe digital environment and enjoy the fruits of the security enhancements brought about by the project. The use of a Voting Classifier, which combines prediction of the DT, the RF, and the SVM, using a soft type of voting method, enhances the effectiveness of the system in detecting and disrupting privilege escalation attacks. An easy to use Flask application that has the SQLite built-in can be used to improve user testing because it has secure signup and signin methods that can ensure a realistic installation and testing.

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

How to cite this article: Krishna Reddy S, Madhavi V. Machine learning-based detection and mitigation of privilege escalation attacks in cloud systems. Int J Drug Deliv Technol. 2026;16(75s): 1615-1621. DOI: 10.25258/ijddt.16.75s.173

I. INTRODUCTION

Cloud computing is the new paradigm of providing and facilitating Internet based services. The infrastructure present. The cloud storage companies also have the necessary security measures to the system and the data that they handle including encryption, access control, and authentication. The cloud has almost unlimited storage of any form of data in or among different storage architectures depending on the perceived accessibility, speed and frequency of accessing data. The intrusion of sensitive information may lead to data breaches due to the large volume of data transferred between the enterprises and cloud service providers, both accidentally and purposefully. The qualities that make the employees and IT systems user-friendly also make the work of firms to prevent unauthorized access hard [2]. Open interfaces and authentication are new IT security challenges that companies face when using cloud services. Hackers with great skills use their knowledge to penetrate into the cloud systems, and ML utilizes various methodologies and algorithms to address security issues and improve data management. There are a lot of datasets relying on privacy concerns and they cannot be leaked, or they might be the ones that do not possess the necessary statistical properties [3], [4].

The fast growth of the Cloud industry introduces the risk of privacy and security that is controlled by the law. The employee access privileges might not be modified when they switch jobs or positions in the Cloud Company. The resultant effect is that outdated privileges are misused with a negative impact of stealing and destroying precious data. All the accounts, which interact with a computer, have some amount of authority. A database in the server, sensitive files and other services are often restricted to authorized users. An attacker may gain access to a vulnerable system by gaining access to a user account with privileged access, and using or expanding it. Attackers can also move horizontally to obtain the control of other systems or vertically to obtain administrative and root access until they dominate the whole environment according to the objectives [1]. Horizontal privilege escalation is the scenario in which the user obtains access privileges of another user with the same access level. A malefactor can use horizontal privilege escalation to acquire information that is not necessarily connected to him or her. Hacker can use a flaw in a poorly developed Web application to find out the personal information of the other people. The attacker has already managed to perform a horizontal privilege escalation exploit, thus they can view, change, and replicate sensitive information.

Hackers target the data repositories because they contain the most valuable and sensitive information. In case of data loss, the privacy and security of all cloud users is jeopardized. Insider threats are harmful activities that are carried out by authorized persons. As networks are growing at an alarming rate, many firms and organizations have come up with an internal network of their own. According to the latest estimates, 9 out of 10 companies feel that they are vulnerable to insider threats. Malefactors can use privilege escalation to develop additional attack vectors to a target system. Attempts of privilege escalation by insider attackers are aimed at gaining higher privileges or access to more sensitive systems. Insider attacks are difficult to identify and counter since they occur under the enterprise level security measures and they usually have privileged access to the network. Recognition and classification of insider threats have become tedious and time consuming.

Research activities conducted recently were oriented towards detection and categorization of privileged elevation attacks committed by insider users. To overcome such challenges, they proposed different ML and DL approaches. Recent works used SVM, Naive Bayes, CNN, Linear Regression, PCA, random forest, and KNN. The need to have fast and high ML algorithms is highly valued due to the diversity of types of attacks. This means that an effective and efficient mechanism is critical in the detection, classification, and alleviation of insider attacks. In order to improve the security protection system, the use of intelligent algorithms, including machine learning algorithms, to classify and predict insider attacks is necessary [17].

Moreover, the knowledge of the effectiveness of machine learning algorithms in detecting insider attacks can be used to select the most appropriate algorithm to be used in a specific case, which requires improvements to the algorithms. This allows the delivery of superior security insurance. This study aims at applying effective and efficient machine learning algorithms in insider attack scenarios in order to achieve better and faster results. The approach to machine learning that has been adopted and evaluated in this respect includes RF, AdaBoost, XGBoost, and LightGBM. The approach by the boosting strategy entails the improvement of a poor classifier to a large extent by increasing the predictions of the classification algorithm. RF, AdaBoost, and XGBoost were effective at classifying insider threats and did this effectively and accurately.

II. Related Work

Cloud computing is the availability of resources of the computer systems on demand. Especially regarding information storage and management feature, which has no direct, singular control on the part of the user. It has provided a single platform through the Internet that provides its clients with public and private computing and data storage. It is also faced with lots of security threats and obstacles that may hinder the embrace of cloud computing technologies. [5]. This paper presents challenges, issues, solutions, and methods of cloud computing security. In a previous poll, a great number of people showed security concerns. The cloud computing architecture approach is also analyzed by another survey, some of which provide information about security issues and policies. All the security concerns, challenges, methodologies and solutions have been consolidated in one location in this article.

Cloud computing refers to the real-time availability of the personal computer system resources especially the data storage and processing capabilities without the involvement of the client. The normal transmission and reception of information among individuals or groups often uses the use of e mails. Phishing is a malicious practice that is often used to steal sensitive data of people on the Internet, pretending to be a legitimate person or organization. 1 Financial data, credit reports, and other sensitive information are often the content of the messages delivered. A phishing email allows the receiver to manipulate the sender to disclose confidential information by deceiving you. The main problem is email phishing attacks in the process of transmission and reception of emails. By email, the assailant sends spam information and gets your data when you open up the email and read it. It has become a big challenge to everybody in the recent years. This research applies different valid and phishing data volumes, recognizes new emails, and makes use of different attributes and algorithms to categorize. An updated data is generated after assessing the existing methodologies. We created feature-extracted CSV file and a label file and applied the SVM [8, 10], NB, and LSTM algorithms [1, 27]. In this experiment, the identification of phished email is considered to be a classification problem. According to the comparison and application, the work of SVM, NB, and LSTM is more accurate and superior in identifying email phishing attacks. Maximum accuracies achieved by the email assaults using SVM, NB and LSTM classifier were 99.62, 97 and 98, respectively.

The next important breakthrough in the sphere is cloud computing that is predetermined by the development of science and technologies. Cloud cryptography refers to a technique that employs encryption as a protection mechanism to ensure the safety of data. The major advantage of the cloud storage is its accessibility, less hardware needs and less cost of maintenance and security and all organizations are now choosing to use cloud. Encryption refers to the process of ciphering information in order to prevent unauthorized access. Now, we are interested in protecting the data stored on our computers or relayed through the internet against attacks. 4 The cryptography methodology depends on speed of reaction, privacy, bandwidth, and integrity. In addition, security is a key factor in the cloud computing to ensure data of clients is stored safely on the cloud. This scientific article assesses the effectiveness, implementation and usefulness of available cryptographic algorithms. The analysis findings reveal what is most appropriate in relation to definite types of data and environment.

The vast use of technology today has resulted in a lot of security issues. Both government and business sectors invest large part of their funds in ensuring that the confidentiality of their data, its integrity and its availability is protected against any form of threat. Insiders attacks are even worse than outsiders as insiders are authorized people who have lawful access to valuable assets of an organization [36]. As a result, many studies in the literature are concerned with the development of methods and instruments to detect and prevent the different types of insider threats. This paper discusses

some of the methods and countermeasures that are suggested to prevent insider attacks. The classification model is suggested to classify insider threat prevention strategies into two different types: the biometric based and the asset based metrics. [36, 37] Biometric based is divided into physiological, behavioral and physical types and asset based is divided into host type, network type and mixed type. This classification is used to categorize the investigated methodologies which are supported by empirical results with the help of the grounded theory technique to conduct a complete literature review. The article also provides comparison and analysis of critical theoretical and empirical variables which have a big effect in determining the effectiveness of the insider threat prevention measures such as datasets, feature domains, classification algorithms, evaluation metrics, real-world simulations, stability and scalability. Major challenges are highlighted that should be overcome during the deployment of real-world systems of insider threat prevention. There are a number of research gaps and suggestions presented on possible research directions.

Internet of things is a transforming technology in which networked computing devices and sensors communicate with each other to analyze diverse problems and the delivery of new services. The enabling technology that is used to make intelligent residences possible is the IoT. Smart home technology has many features to users such as temperature sensors, smoke sensors, automatic lights and smart locks. However, it also leads to a new set of security and privacy issues; one of them is the fact that the personal information of people can be exposed by manipulating the surveillance systems or creating false fire alarms and so forth. These issues make smart homes susceptible to various security risks, which make people unwilling to implement this new technology because of safety concerns. This survey report [6] explains what is the IoT, how it grows, what are the objects standards used by the environment, the layered architecture of the IoT environment and the various security issues that are present in each of the layers applied in the smart home. The research paper outlines the difficulties and problems encountered in smart homes due to the implementation of IoT in addition to giving means of alleviating these security threats.

III. Materials And Methods

i) Proposed Work:

The proposed system is a machine learning based approach to the detection and classification of insider threats in the cloud environment. RF, Adaboost, XGBoost and LightGBM algorithms can be used to enhance predictive performance. The proposed approach will improve the precision of detecting insider threats through the application of different machine learning models, including Random Forest, Adaboost, XGBoost, and LightGBM. The system utilizes the ensemble learning methods to combine the capabilities of numerous algorithms and thus enhances the accuracy of predictions of insider threats in the clouds. The system employs elaborate data pretreatment procedures, such as aggregation and normalization, to address the problems of missing values, outliers, and outlier features, thus improving the performance of the model. Such parameters as learning rate, the maximal depth, and K-fold are tuned to improve the effectiveness of machine learning models that will help identify insider threats with a more efficient and personalized approach. And also a Voting Classifier that combines predictions of DT, RF and SVM [10] using a soft method of voting also improves the performance of the system against privilege escalation attacks. An easy-to-use Flask application and SQLite interconnection provide greater user testing as it implements secure signup and signin that can be used to install and test its functionality in a real-life scenario.

ii) System Architecture:

The system architecture is made up of four basic steps, including data collecting, data preprocessing, the implementation of monitored machine learning algorithms, and the results analysis. In the data collection period, a customized dataset obtained in different files of the CERT database is used. Subsequently, the resulting data undergoes preprocessing, which consists of such techniques as the aggregation of data, data normalization, and feature extraction in order to enhance its quality and relevance. The architecture of the system implies the use of ML algorithms, such as the Random Forest, AdaBoost, XGBoost, and LightGBM, and a voting classifier as an improvement, which will be applied to the processed data to detect and classify the threat of privilege escalation. The system performs an in-depth analysis of the findings, evaluating the performance of each algorithm, and providing a clue on the effectiveness of the whole system in terms of identifying insider threats. This architecture will ensure a systematic and robust approach to privilege escalation assault reduction through machine learning techniques.

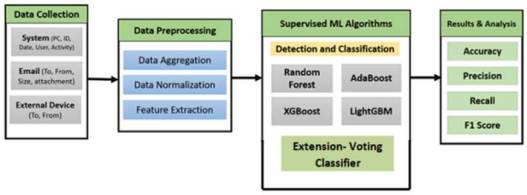


Fig. 1. System Architecture

iii) Dataset collection:

The data that was used in this experiment is obtained through a number of files in the CERT dataset [13, 14], and the focus is on the email related data. The dataset is a selection of cases that are relevant to insider threat situations in email communications. It includes a number of factors and characteristics related to user actions, email messages, and interactions with the system.

	id	date	user	pc	to	cc	bcc	
0	{R3I7-S4TX96FG-8219JWFF}	01/02/2010 07:11:45	LAP0338	PC-5758	Dean.Flynn.Hines@dtaa.com;Wade_Harrison@lockhe...	Nathaniel.Hunter.Heath@dtaa.com	NaN	Lynn.Adena.Pr
1	{R0R9-E4QL59IK-2907OSIWJ}	01/02/2010 07:12:16	MOH0273	PC-6699	Odonnell-Gage@bellsouth.net	NaN	NaN	MOH68(
2	{G2B2-A8XY58CP-2847ZJZL}	01/02/2010 07:13:00	LAP0338	PC-5758	Penelope_Colon@netzero.com	NaN	NaN	Lynn_A_Prath
3	{A3A9-F4TH89AA-8318GFGK}	01/02/2010 07:13:17	LAP0338	PC-5758	Judith_Hayden@comcast.net	NaN	NaN	Lynn_A_Prath
4	{E8B7-C8F288UF-2946RUOQ}	01/02/2010 07:13:28	MOH0273	PC-6699	Bond-Raymond@verizon.net;Alea_Ferrell@msn.com;...	NaN	Odonnell-Gage@bellsouth.net	MOH68(

Fig. 2 CERT dataset

iv) Data Processing:

Data processing is transforming raw data to useful information to companies. Data scientists are usually involved in data processing, which involves the gathering, structuring, cleaning, ensuring data accuracy, as well as data processing and transformation into understandable formats, e.g. graphs or papers. There are three data processing procedures namely, manual, mechanical and electronic. This is aimed at increasing information value and simplifying decision making. This enables businesses to improve on their operations and make quick strategies. This is dependent on automated data processing technology such as computer software programming. It can process large volumes of data, particularly, the big data, into meaningful intelligence to quality management and decision-making.

v) Feature selection:

The process of picking out the most consistent, non-redundant and relevant features to the model development is known as feature selection. Reducing the size of the dataset systematically is essential at the time when the size and diversity of datasets continue to grow. The main aim of feature selection is to optimize the effectiveness of a predictive model and reduce the cost of modeling in terms of computational costs.

A fundamental feature engineering task is feature selection; that is, which features to be considered the most important in feeding into machine learning algorithms. The process of feature selection is applied to the input variables to reduce the number of redundant or irrelevant variables, therefore, narrowing down the number of input variables to those most relevant to the machine learning model. The main benefits of doing feature selection prior to it being left to the machine learning model to decide which characteristics are important.

vi) Algorithms:

LightGBM: LightGBM is an ensemble method of gradient boosting used by the Train Using AutoML tool, which is based on decision trees. Like other decision tree-based methods, LightGBM can also be used on both classification and regression. LightGBM is also designed to work in a distributed system (optimally) [31, 32].

XGBoost: XGBoost is a popular, and successful open-source package of the gradient boosting trees method. Gradient boosting is a supervised learning model, which aims at accurately predicting a target variable by combining the predictions of a group of smaller and weaker models.

AdaBoost: Adaptive Boosting or AdaBoost is a machine learning system that is used as an Ensemble Method. A single level decision tree, which implies a decision tree having a single split, is the most common estimator used in AdaBoost. These are known as Decision Stumps.

RF: Random forest is a ML method that is highly used and patented by Leo Breiman and Adele Cutler and involves combining the results of a large number of decision trees to obtain a single result. Its ease of use and flexibility have contributed to its adoption, because it can be used to solve classification and regression problems [34].

VC: A Voting Classifier is a machine learning model which is trained on a group of many models and makes its prediction by selecting an output (class) based on its had-most-probability of the selected class being the output.

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:

$$Accuracy = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{FP} + \mathrm{TN} + \mathrm{FN}} (3)$$

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:

$$Precision = \frac{\text{True Positive}}{\text{True Positive } + \text{False Positive}} (4)$$

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.

$$Recall = \frac{\mathrm{TP}}{\mathrm{TP} \ + \ \mathrm{FN}} (5)$$

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.

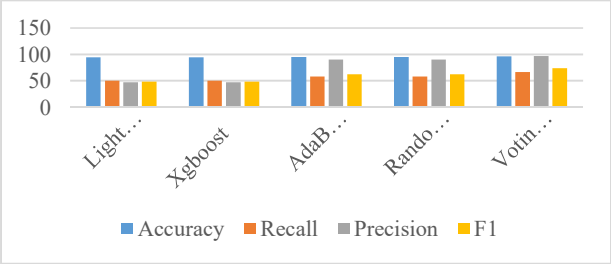
$$F1\ Score = 2 * \frac{Recall \ \mathrm{X}\ Precision}{Recall + Precision} * 100 (6)$$

Table. 1. Performance Evaluation

Model Name	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

Table (1) compares the performance metrics of the two methods Accuracy, Precision, Recall and F1 Score. The Voting Classifier is consistently ranked higher than all other algorithms in all measurements. The tables give a comparative analysis of the measures of the alternative methods.

Graph.1 Comparison Graph For Performance Evaluation



Graph (1) represents accuracy as blue, precision as gray, recall as orange and F1-Score as yellow. As compared to the other models, Voting Classifier has a better performance on all measures showing the highest values. These findings are described in the graphs above.

Fig 3 Home Page

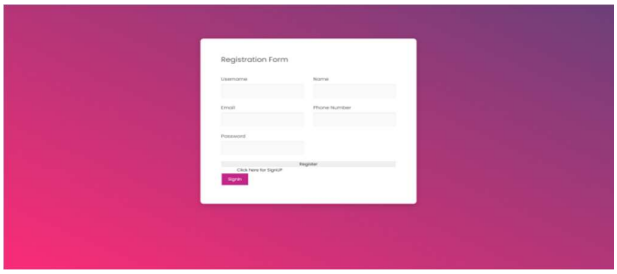


Fig 4 Signup Page

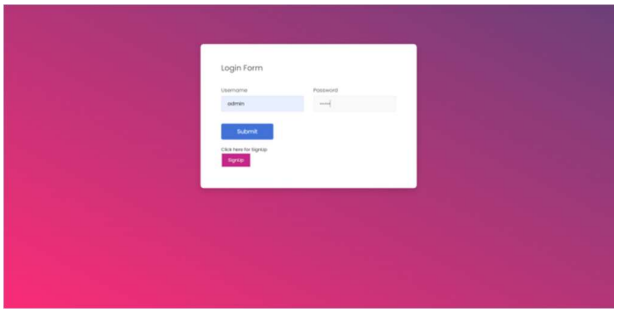


Fig 5 Signin Page

Fig 6 User input Page

Fig 7 Prediction Result

V. CONCLUSION

The evil insider is a significant threat to the business as he or she has greater access and opportunity to cause significant damage. The knowledge and resources are available to insiders in a very exclusive and suitable manner in contrast to outsiders. This paper gives machine learning algorithms to detect and classify insider attacks. [14]. This work relies on a custom dataset obtained based on a number of files of the CERT dataset. On the dataset, four machine learning techniques were used, which gave the best results. The algorithms are RF, AdaBoost, XGBoost and LightGBM. The current study had very good results in the experimental work with higher accuracy in categorization in the report of the categorization with supervised machine learning. Among the suggested algorithms, LightGBM has the greatest accuracy of 97 percent; the accuracy of the rest of the algorithms is as follows: RF 86 percent, AdaBoost 88 percent, and XGBoost 88.27 percent [31, 32]. The proposed models could be improved in the future by increasing the size and diversity of the dataset in terms of its characteristics and the newly developed trends of insider attackers. This can be used to open new research horizons in detection and classification of insider attacks in most organizational areas. Machine learning models are used by businesses to enable them to make informed decisions, and improved outcomes of these models lead to better judgments. The cost of error is high; however, this cost is reduced through improved accuracy of the model. The research based on machine learning enables users to feed large volumes of data in the computer algorithms which then analyze, propose and make a decision of the data presented.

VI. FUTURE SCOPE

The future should focus on enhancing the scale of the system to handle more work in large clouds efficiently and thus deliver a smooth processing even when the data complexity and volume go up. New technology should be able to include new dynamic reactions which can easily identify and neutralize any emerging strategies in the privilege-escalation attacks and thus provide a proactive protection against an increasing insider threat. It is essential to include ways that provide intelligible arguments regarding how the models are arrived at. This openness helps security analysts to learn the factors that influence the process of detecting threats, therefore, increasing confidence in the outcomes of the machine [29, 30]. A system of continual updating and diversity of the set used to train the models should be offered. Constant improvement ensures the

effectiveness of the system in identifying and neutralizing new attack vectors and new trends 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] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, ''On the effectiveness of machine and deep learning for cyber security,'' in Proc. 10th Int. Conf. Cyber Conflict (CyCon), May 2018, pp. 371–390.

[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] X. Sun, Y. Wang, and Z. Shi, ''Insider threat detection using an unsupervised learning method: COPOD,'' in Proc. Int. Conf. Commun., Inf. Syst. Comput. Eng. (CISCE), May 2021, pp. 749–754.

[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] L. Liu, O. de Vel, Q.-L. Han, J. Zhang, and Y. Xiang, ''Detecting and preventing cyber insider threats: A survey,'' IEEE Commun. Surveys Tuts., vol. 20, no. 2, pp. 1397–1417, 2nd Quart., 2018.

[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] G. Ravikumar and M. Govindarasu, ''Anomaly detection and mitigation for wide-area damping control using machine learning,'' IEEE Trans. Smart Grid, early access, May 18, 2020, doi: 10.1109/TSG.2020.2995313.

[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] L. Coppolino, S. D'Antonio, G. Mazzeo, and L. Romano, ''Cloud security: Emerging threats and current solutions,'' Comput. Electr. Eng., vol. 59, pp. 126–140, Apr. 2017.

[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] N. Alhebaishi, L. Wang, S. Jajodia, and A. Singhal, ''Modeling and mitigating the insider threat of remote administrators in clouds,'' in Proc. IFIP Annu. Conf. Data Appl. Secur. Privacy. Bergamo, Italy: Springer, 2018, pp. 3–20.

[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] P. Kaur, R. Kumar, and M. Kumar, ‘‘A healthcare monitoring system using random forest and Internet of Things (IoT),’’ Multimedia Tools Appl., vol. 78, no. 14, pp. 19905–19916, 2019.

[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.