International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

LEVERAGING MACHINE LEARNING FOR DETECTING AND COUNTERING PRIVILEGE ESCALATION ATTACKS IN CLOUD

Angiti Pratyusha, Mr.N.Naveen Kumar

M tech(Computer Science),Student, Department of Information Technology, Associate Professor of CSE, JNTUHUCESTH, Hyderabad, Telangana – 500085

Abstract: I propose utilizing modern ML to reinforce cloud security, with an emphasis on distinguishing and defeating honor heightening dangers to make a more grounded cautious. Honor heightening assaults are turning out to be more normal as cloud use increments. To work on by and large security, this undertaking handles shortcomings in representative access honors inside cloud administrations. The task takes into consideration the continuous recognition and relief of honor acceleration dangers through the use of ML. Systems like Adaboost, Xgboost, Random Forest, and LightGBM assist with giving a unique protection against continually evolving dangers. Organizations and clients benefit from expanded information security, which increments trust in distributed computing. The undertaking's expanded security benefits cloud specialist organizations and organizations by giving them more confidence in a safe web-based climate. Moreover, a "soft" voting technique Voting Classifier is added, which consolidates forecasts from Random Forest, Decision Tree, and Support Vector Machine to work on the framework's capacity to distinguish and moderate honor heightening attacks. Moreover, a simple to-utilize Flask system incorporated with SQLite improves client testing by offering safe information exchange and signin highlights for certifiable application and assessment.

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

1. INTRODUCTION

Cloud computing is a new way of thinking about how to facilitate and provide services through the Internet. The current infrastructure. Cloud storage providers adopt fundamental security measures for their systems and the data they handle, including encryption, access control, and authentication. Depending on the accessibility, speed, and frequency of data access, the cloud has an almost infinite capacity for storing any type of data in different cloud data storage structures. Sensitive data breaches might occur due to the volume of data that moves between businesses and cloud service providers, both inadvertent and malicious. The

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

characteristics that make online services easy to use for workers and IT systems also make it harder for businesses to prevent unwanted access [2]. Authentication and open Interfaces are new security vulnerabilities that Cloud services subject enterprises face. Hackers with advanced skills utilize their knowledge to access Cloud systems Machine learning employs a variety of approaches and algorithms to address the security challenge and better manage data. Many datasets are private and cannot be released owing to privacy concerns, or they may be missing crucial statistical properties [3], [4].

The fast rise of the Cloud industry creates privacy and security risks governed by regulations. Employee access privileges may not necessarily change when they change roles or positions within the Cloud Company. As a result, old privileges are used inconveniently to steal and harm valuable data. Each account that communicates with a computer has some level of authority. Server databases, confidential files, and other services are often restricted to approved users. A malicious attacker can access a sensitive system by gaining control of a higher user account and exploiting or expanding privileges. Based on their objectives, attackers can move horizontally to obtain control of more systems or vertically to obtain admin and root access till they have complete control of the whole environment [1]. When a user gets the access permissions of another user with the same access level, this is known as horizontal privilege escalation. An attacker can use horizontal privilege escalation to access data that does not necessarily relate to him. An attacker may be able to uncover holes in a Web application that provides him entry to certain other people's information in badly designed apps [3], [5]. Because the attacker has completed a horizontal elevation of privileges exploit, they can see, alter, and copy sensitive information.

Attackers target data sources because they have the most valuable and sensitive information. Every cloud user's privacy and security are affected if data is lost. Insider threats are harmful operations carried out by people with authorization. With the fast growth of networks, many companies and organizations have established their internal networks. According to recent estimates, 90% of businesses believe they are vulnerable to insider assaults [7]. Attackers can use privilege elevation to open up additional attack routes on a target system. Insider attackers try to get higher privileges or access to more sensitive systems by attempting privilege escalation. Insider attacks are difficult to identify and prevent because they exist beneath the enterprise-level security defense measures and frequently have privileged access to the network. Detecting and classifying insider threats has become difficult and time-consuming [8].

In recent studies, researchers worked on detecting and classifying privileged elevation attacks from insider personnel. They proposed different machine learning and deep learning techniques to counter these challenges. Techniques like SVM, Naïve Bayes, CNN, Linear Regression, PCA, Random Forest, and KNN were applied in recent studies. However, the demand for fast and effective machine learning algorithms is highly valued with the diversity of attack types. Therefore an effective and efficient strategy is required to detect, classify and mitigate these insider

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

attacks. To get better security protection systems, we need intelligent algorithms, such as ML algorithms, to classify and predict insider attacks [17].

In addition, knowing the performance of ML algorithms on classifying insider attacks allows you to choose the most appropriate algorithm for each case, and the ones (ML algorithms) need to be improved. So you can provide a higher level of security protection. This research aims to apply effective and efficient ML algorithms to insider attack scenarios to gain better and faster results. ML algorithms have been applied and evaluated in this regard: Random Forest, AdaBoost, XGBoost, and LightGBM. The principle behind the boosting strategy is to take a weak classifier and train it to become a very good one by raising the prediction of the classification algorithm. Random Forest, AdaBoost, and XGBoost worked accurately and quickly to classify insider threats.

2. LITERATURE REVIEW

Cloud computing is the on-demand availability of PC framework resources. Especially information storage and handling power, without direct unique administration by the customer. It has provided customers with public and private computing and data storage on a single platform across the Internet. Aside from that, it faces several security threats and issues, which may slow down the adoption of cloud computing models. [5] Cloud computing security threats, difficulties, strategies, and solutions are discussed in this paper. Numerous people raised security concerns in a previous survey. Another survey looks at the cloud computing architectural model, and a few of them detail security challenges and techniques. This article brings together all the security concerns, difficulties, techniques, and solutions in one place.

Cloud computing refers to the on-demand availability of personal computer system assets, specifically data storage and processing power, without the client's input. Emails are commonly used to send and receive data for individuals or groups. Financial data, credit reports, and other sensitive data are often sent via the Internet. [1] Phishing is a fraudster's technique used to get sensitive data from users by seeming to come from trusted sources. The sender can persuade you to give secret data by misdirecting in a phished email. The main problem is email phishing attacks while sending and receiving the email. The attacker sends spam data using email and receives your data when you open and read the email. In recent years, it has been a big problem for everyone. This paper uses different legitimate and phishing data sizes, detects new emails, and uses different features and algorithms for classification. A modified dataset is created after measuring the existing approaches. We created a feature extracted comma-separated values (CSV) file and label file, applied the support vector machine (SVM) [8, 10], Naive Bayes (NB), and long short-term memory (LSTM) algorithm [1, 27]. This experimentation considers the recognition of a phished email as a classification issue. According to the comparison and implementation, SVM, NB and LSTM performance is better and more accurate to detect email phishing attacks. The classification of email attacks using SVM, NB, and LSTM classifiers

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

achieve the highest accuracy of 99.62%, 97% and 98%, respectively.

With advancements in science and technology, cloud computing is the next big thing in the industry. Cloud cryptography is a technique that uses encryption algorithms to secure data [4]. The significant advantage of cloud storage is no difficulty to get to, diminished equipment, low protection, and fixing cost so every association is working with the cloud. Encryption is the process of encoding information to prevent unauthorized access. Nowadays, we desire to secure the information that is to be stored in our computer or transmitted utilizing the internet against attacks. [4] The cryptographic method depends on their response time, confidentiality, bandwidth, and integrity. Furthermore, security is a significant factor in cloud computing for ensuring client data is placed on the safe mode in the cloud. Our research paper compares the efficiency, usage, and utility of available cryptography algorithms. Evaluation results suggest which algorithm is better for which type of data and environment.

With the wide use of technologies nowadays, various security issues have emerged. Public and private sectors are both spending a large portion of their budget to protect the confidentiality, integrity, and availability of their data from possible attacks. Among these attacks are insider attacks which are more serious than external attacks, as insiders are authorized users who have legitimate access to sensitive assets of an organization [36]. As a result, several studies exist in the literature aimed to develop techniques and tools to detect and prevent various types of insider threats. This article reviews different techniques and countermeasures that are proposed to prevent insider attacks. A unified classification model is proposed to classify the insider threat prevention approaches into two categories (biometric-based and asset-based metric). [36, 37] The biometric-based category is also classified into (physiological, behavioral and physical), while the asset metric-based category is also classified into (host, network and combined). This classification systematizes the reviewed approaches that are validated with empirical results utilizing the grounded theory method for rigorous literature review. Additionally, the article compares and discusses significant theoretical and empirical factors that play a key role in the effectiveness of insider threat prevention approaches (e.g., datasets, feature domains, classification algorithms, evaluation metrics, real-world simulation, stability and scalability, etc.). Major challenges are also highlighted which need to be considered when deploying real-world insider threat prevention systems. Some research gaps and recommendations are also presented for future research directions.

The Internet of Things [34] is a rapidly evolving technology in which interconnected computing devices and sensors share data over the network to decipher different problems and deliver new services. For example, IoT is the key enabling technology for smart homes. Smart home technology provides many facilities to users like temperature monitoring, smoke detection, automatic light control, smart locks, etc. However, it also opens the door to new set of security and privacy issues, for example, the private data of users can be accessed by taking control over

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

surveillance devices or activating false fire alarms, etc. These challenges make smart homes feeble to various types of security attacks and people are reluctant to adopt this technology due to the security issues. In this survey paper [6], we throw light on IoT, how IoT is growing, objects and their specifications, the layered structure of the IoT environment, and various security challenges for each layer that occur in the smart home. This paper not only presents the challenges and issues that emerge in IoT-based smart homes but also presents some solutions that would help to overcome these security challenges.

3. METHODOLOGY

i) Proposed Work:

The proposed framework is an ML based way to deal with ordering and distinguishing insider dangers in cloud settings. Forecast execution is improved by utilizing the Random Forest, Adaboost, XGBoost, and LightGBM calculations. further consolidated a Voting Classifier, which works on the framework's presentation in recognizing and upsetting honor heightening endeavors by joining forecasts from Decision Tree, Random Forest, and Support Vector Machine [10] through a "delicate" casting a ballot procedure. Besides, an easy to-utilize flask system incorporated with SQLite improves client testing by offering secure information exchange and signin highlights for genuine application and evaluation.To all the more accurately distinguish and sort insider dangers, we are applying the five troupe models to a solitary, exceptionally made dataset. The best results of utilized gathering calculations were displayed in our review.

ii) System Architecture:

The system architecture comprises four key stages: data collection, data preprocessing, application of supervised machine learning algorithms, and results analysis. In the data collection phase, a customized dataset derived from multiple files of the CERT dataset is utilized. Subsequently, the collected data undergoes preprocessing, involving techniques such as data aggregation, normalization, and feature extraction to enhance its quality and relevance. The core of the system involves applying machine learning algorithms—Random Forest, AdaBoost, XGBoost, and LightGBM [31, 32] and a voting classifier as an extension—to the preprocessed data for the detection and classification of privilege escalation attacks. Finally, the system conducts a thorough analysis of the results, evaluating the performance of each algorithm and providing insights into the effectiveness of the overall system in identifying insider threats. This architecture ensures a systematic and robust approach to addressing privilege escalation attacks through machine learning techniques.

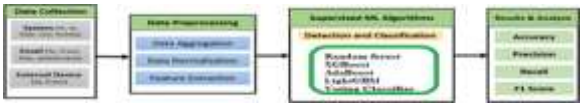

Fig 1 Proposed architecture

iii) Dataset collection:

The dataset employed in this project is derived from multiple files within the CERT dataset [13, 14],

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

specifically focusing on email-related information. This curated dataset captures a variety of instances relevant to insider threat scenarios within email communications. It includes diverse features and attributes related to user behavior, email content, and system interactions.

Fig 2 CERT dataset

iv) Data Processing:

Data processing involves transforming raw data into valuable information for businesses. Generally, data scientists process data, which includes collecting, organizing, cleaning, verifying, analyzing, and converting it into readable formats such as graphs or documents. Data processing can be done using three methods i.e., manual, mechanical, and electronic. The aim is to increase the value of information and facilitate decision-making. This enables businesses to improve their operations and make timely strategic decisions. Automated data processing solutions, such as computer software programming, play a significant role in this. It can help turn large amounts of data, including big data, into meaningful insights for quality management and decision-making.

v) Feature selection:

Feature selection is the process of isolating the most consistent, non-redundant, and relevant features to use in model construction. Methodically reducing the size of datasets is important as the size and variety of datasets continue to grow. The main goal of feature selection is to improve the performance of a predictive model and reduce the computational cost of modeling.

Feature selection, one of the main components of feature engineering, is the process of selecting the most important features to input in machine learning algorithms. Feature selection techniques are employed to reduce the number of input variables by eliminating redundant or irrelevant features and narrowing down the set of features to those most relevant to the machine learning model. The main benefits of performing feature selection in advance, rather than letting the machine learning model figure out which features are most important.

vi) Algorithms:

LightGBM: The Train Utilizing AutoML instrument utilizes LightGBM, a slope helping gathering approach in view of decision trees. LightGBM is a choice tree-based strategy that might be applied to relapse as well as characterization. Elite execution with dispersed frameworks is the focal point of LightGBM's streamlining.

XGBoost: The slope helped trees approach is a popular and successful open-source execution, and Amazon SageMaker XGBoost makes sense of how it works. Slope supporting is a regulated learning approach that joins the evaluations of a few more vulnerable, easier

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

models with an end goal to foresee an objective variable with a serious level of exactness.

AdaBoost: Otherwise called Versatile Helping, AdaBoost is an ML outfit technique procedure. Decision trees with one level, or Decision trees with just a single split, are the most well known assessor utilized with AdaBoost. One more name for these trees is Decision Stumps.

RF: Leo Breiman and Adele Cutler are the brand name holders of the generally utilized ML procedure known as "random forest," which totals the result of a few Decision trees to create a solitary end. Its flexibility and convenience, joined with its capacity to deal with both relapse and arrangement issues, have driven its prominence.

VC(RF+SVM+DT): A Voting Classifier, or VC(RF+SVM+DT), is a sort of ML model that gains from an outfit of many models and predicts a result (class) in view of the models' best probability of creating the ideal class. To work on generally execution and accuracy, we are consolidating the predictions of Random Forest, Support Vector Machine, and Decision Tree using this technique.

4. EXPERIMENTAL RESULTS

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 = True positives/ (True positives + False positives) = TP/(TP + FP)

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

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.

$$Recall = \frac{TP}{TP + FN}$$

Accuracy: Accuracy is the proportion of correct predictions in a classification task, measuring the overall correctness of a model's predictions.

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

F1 Score: The F1 Score is the harmonic mean of precision and recall, offering a balanced measure that considers both false positives and false negatives, making it suitable for imbalanced datasets.

$$\text{F1 Score} = 2 * \frac{\text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}} * 100$$

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

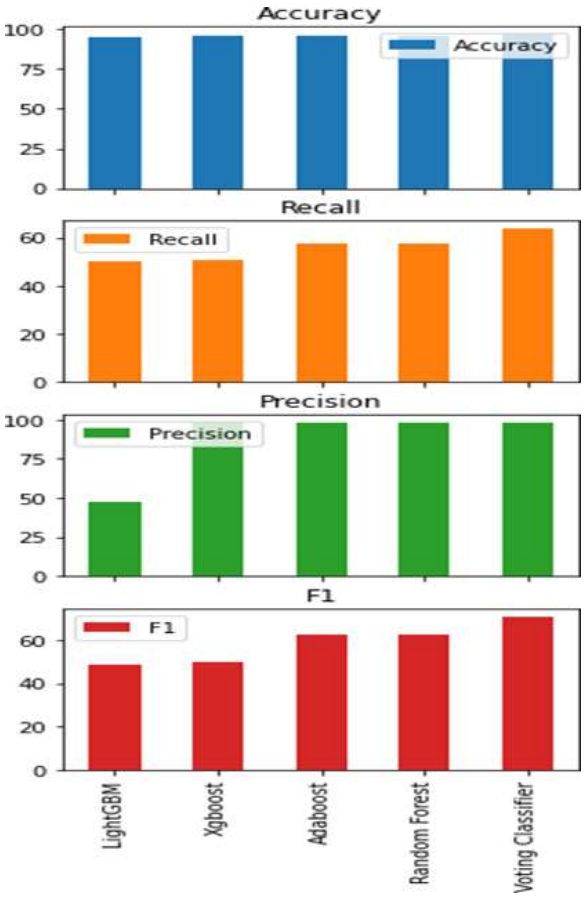

Fig 3 : Performance evaluation

Fig 4 : Home Page

Fig 5 : Signup Page

Fig 6 :Signin Page

Fig 7 : Main Page

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

Fig 8 : User input Page

Fig 9 : Prediction Result

Fig 10: Upload Another Message

Fig 11: Final Outcome

5. CONCLUSION

Because of their expanded admittance and potential for serious mischief, pernicious insiders represent a serious danger to the organization. Insiders have suitable and restricted admittance to information and assets, as opposed to outcasts. The ML strategies for recognizing and arranging insider assaults were introduced in this work. In this work, a changed dataset made out of many records from the CERT dataset is utilized. At the point when five ML strategies were utilized on that dataset, the results moved along. Random Forest, AdaBoost, XGBoost, Voting Classifier, and LightGBM are these calculations. This study utilized these administered ML techniques to show how fruitful the trial discoveries were as far as classification report accuracy . The Voting Classifier technique, out of the relative multitude of proposed calculations, has the best accuracy (96%); the other exactness scores are 94% for RF, 95% for AdaBoost, 94% for LightGBM, and 94% for XGBoost. This could prompt new review bearings in the distinguishing proof and classification of insider dangers across a great many hierarchical spaces. Organizations use ML models to pursue credible business choices; better model discoveries convert into

better choices. Despite the fact that mistakes could have a huge monetary effect, this cost can be diminished by expanding model exactness. With ML research, clients might take care of huge volumes of information to PC calculations, which use the information to survey, recommend, and decide.

6. FUTURE SCOPE

Future enhancements should focus on optimizing the system's scalability to efficiently handle increased workloads in expansive cloud setups, ensuring smooth processing even as data complexity and volume grow. Future developments should implement dynamic response mechanisms capable of rapidly identifying and countering newly emerging tactics in privilege escalation attacks, providing a proactive defense against evolving insider threats. The integration of techniques that provide understandable explanations for model decisions is essential. This transparency helps security analysts comprehend the factors influencing threat identifications, fostering trust in the system's outputs [29, 30]. Establishing a framework for continuously updating and diversifying the dataset used for training the models is crucial. Ongoing enrichment ensures the system's effectiveness in identifying and mitigating new types of attacks and evolving insider threat patterns.

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.