Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 6, No.3, June : 2025

UNMASKING THE INSIDER: DEEP LEARNING-BASED THREAT DETECTION IN CLOUD PLATFORMS

J. VidhyaJanani, Assistant Professor, Department of Computer Science and Engineering, Paavai College of Engineering, Namakkal.
D. Devadharshini, Student**,** Department of CSE (Artificial Intelligence and Machine Learning), Paavai College of Engineering, Namakkal
M. Hema, Student**,** Department of CSE (Artificial Intelligence and Machine Learning), Paavai College of Engineering, Namakkal
S. Ranjani, Student**,** Department of CSE (Artificial Intelligence and Machine Learning), Paavai College of Engineering, Namakkal
M. Shamini, Student**,** Department of CSE (Artificial Intelligence and Machine Learning), Paavai College of Engineering, Namakkal
P. Priyadharshini, Student**,** Department of CSE (Artificial Intelligence and Machine Learning), Paavai College of Engineering, Namakkal
R. Bharath Kumar, Student**,** Department of CSE (Artificial Intelligence and Machine Learning), Paavai College of Engineering, Namakkal
M. Vinoth, Student**,** Department of CSE (Artificial Intelligence and Machine Learning), Paavai College of Engineering, Namakkal

Abstract
Users, owners, third-party users, authorized users, and customers can quickly access and store their information thanks to cloud computing's high network infrastructure. The use of cloud computing has made people aware of the need for a centralized location for efficient processing and the rapid increase in information in all fields. These days, internal user threats have a significant impact on this cloud. Real user threats are more likely to affect sensitive applications like banking, hospital, and business. An intruder is set up as a member of the network and presented as a user. They will attempt to attack or steal sensitive data during information sharing or conversation once they become inside the network. The significant issue in the present mechanical advancement is recognizing the insider danger in the cloud organization. At the point when information is lost, compromising cloud clients is difficult. Because privacy and security aren't guaranteed, people don't trust using the cloud. For the cloud network's external security, there are a number of options. However, it is necessary to deal with internal or inside threats. In this study, we concentrate on a technique for using artificial intelligence to identify an insider attack. An insider assault is conceivable by utilizing hubs of feeble clients' frameworks. They will connect to a network and pretend to be a trusted node before logging in with a weak user ID. As an insider, they can then easily attack and hack information, making identification extremely challenging. Intelligent responses are required for attacks of this kind. For security concerns, a machine learning approach is frequently utilized. Until this point in time, the current slacks can arrange the assailants precisely. Young researchers are motivated to offer a solution to internal threats because the information hijacking process is so absurd. Using a user interaction behavior pattern and deep learning, we track the attackers in our proposed work. A database stores the actual user's mouse clicks, keystrokes, and mouse movements. Using a restricted Boltzmann machine (RBM), the deep belief neural network's RBM layer communicates with the preceding and subsequent layers. A cloud-based Cooja simulator is utilized for the evaluation of the outcome.

Keywords:
Machine Learning, Cyber attacks, Cloud security, Intrusion Detection System.

I. Introduction

The information technology (IT) world has a new revolution technology called cloud computing. A

cloud infrastructure has many benefits, such as dynamic resource utilization, on-demand storage processing, and sharing unlimited resources. Cloud computing is creating a new revolution in the IT sector, but security is the major problem. The network security is highly affected by outsider and insider intruders. Providing external security is very easy, but internal security is a very difficult task. Internal intruders are pretending to be real users in the network. They tend to use authorized nodes and collapse the entire cloud network by attacking sensitive information [1]. External security has advanced firewall software to protect the system from outsider threats. When compared with an external threat, an insider attack is the most dangerous one. Insider attacks take place by following loopholes, such as using an authorized node or attacking using an authorized ID or malicious attack pretending to be a trusted node or stealing sensitive information as a user. If an intruder is present in the cloud network, then the intruder lays a way for other malicious nodes to enter the network. Recently, several studies on security threats in cloud computing exist.

In this research article, we consider abnormal behavior as a threat. However, such an abnormal behavior may have some reasons, such as a broken node that cannot work normally. Identifying malicious behavior is very challenging among insider attacks. Hackers inside the network look for the weakest node and then attack the sensitive data in the cloud server. Authorized user attackers as an insider affect the cloud network in privacy preservation. They pretend to a real user and obtain all legal services from the cloud service provider. These problems of internal attack are currently handled using various machine learning (ML) approaches. Organizations face most damages on reputation, financial data, and enterprise property because of internal threats. As of the 2018 report, 53% of the attack happens because of insider hacking, and 28% are internal attackers adjudged as an organization origin [2,3]. The leakage of data statistics conducted states that many internal or insider threats are noticed by the media. The big solution from most organizations tends to buy or design powerful firewalls, cyber techniques, intrusion identification, and digital monitoring system to identify insider threats. Identifying the wrong or malicious nodes in the organization is possible using the threat detection technique. This technique provides mitigation measures and detection before attacking. Whatever technology precipitates, identifying and understanding insider attacks are difficult. Every existing technique has some limitations, and many solutions fail to detect exact insiders. Therefore, studying the limitation of existing internal attack algorithms and identifying the solution for limitations are necessary. Recently, ML and deep learning techniques provide a solution for most security issues in the cloud network. Among them, identification of user behavior in various perspectives is highly motivated to obtain a better solution. The best-case study of insider threats includes one of the famous problem cases in Wiki Leaks on July 25, 2010, where a diary during the Afghan war is released as a document containing more than 90,000 reports. The diary describes the Afghan war from 2004 to 2010. This leakage is caused by an insider army of the US. He is a worker in army analytic in the intelligence department, making government communities and business organizations pay attention to insider threats. The “insider threat” among scholars is defined as an authorized access node misused by an authorized user to harm or other intentions. Many ML techniques focus on determining a negative intention. A spammer user identification method is an ML approach used to learn the behavior of the user in the cloud network [4]. The collected behavior is classified using deep learning technology. The training layer detects the behavior and classifies them as a normal or abnormal user. To date, cloud service providers have not provided adequate datasets in real time. Considering the confidential data process, we cannot obtain real datasets. Hence, we use supervised algorithms to look for real datasets for training the model. Training the model without a proper dataset is very insufficient and hard. Moreover, unsupervisedlearning does not require pre-training of dataset in the training model but takes input data at a time and trains the model automatically during the process.

II. Literature Review

External threats are greatly influenced by internal attack detection techniques. The detection of an internal threat is fully based on the strategy of overflowing using a buffer [5]. An internal threat does

not provide efficient metrics for the testing environment. Testing on real data has a very limited measure. The traditional insider attack detection can be classified as host-based, networking-based, and informationbased detections. The user behavior of the host nodes is monitored in this research article. Host-based intruder detection is conducted by monitoring the user behavior pattern. First, the behavior pattern is recorded, and ML techniques are used to detect the changes in the normal behavior pattern. The supervised and unsupervised learning methods are used. To detect an insider attack, biometric data play a major role in the authentication process nowadays [6]. The user biometric details and psychological character are stored as testing data.

Psychological characteristics such as iris and fingerprint are used. Behavioral data are nothing but mouse movement and click and keystroke patterns of the users. In most detections, physiological biometric data have poor processing applicability and is as simple as password hacking. Keystroke-based internal threat detection is first proposed in 1999. Some behavior characteristics of the user attract attention for security purposes, and scholars tend to pay more attention to such characteristics for threat detection.

The different anomaly detection techniques [7,8] using mouse patterns are discussed. The patterns are based on mouse movement angle, distances moved, acceleration performed, and others, and keystroke patterns include stroking interval, duration, and valued pairs. A system based on the European standard [9] for present threat detection techniques on user behavior has a problem with high accuracy. To date, these techniques cannot meet the requirement of security concerns. In most of the present techniques, the output of the false alarm rate is very high. Notably, existing research focused on biological identification as security characteristics. Biological identification is considered an abnormal system model because of lagging in a high-threat detection strategy. These methods consider that the user behavior pattern is very difficult and less potential tasks. Authenticating the user is considered a text classification problem by processing system commands [10]. Here, they use an n-gram framework to process word sequences.

The parameters of the system call include the status of processing data and values of results. The system and user calls tend to establish a relationship between the user and process for threat detection [11]. The hidden Markova model is a dynamic method [12] with the distributive static model combined to detect anomalies in the network. The process of detection is based on the system call by monitoring all the activities on the host side. During the detection process, an overhead by different threat behaviors exists, which leads to the highest false reading. To overcome the above problems, that is, large data log process and drifting problems in training data, article [13] proposed a technique based on the training data set.

A user of this model tends to store its access behavior and characteristics. This behavior pattern is stored as sequences for processing the queries. This technique provides great advantages by reducing a load of data and continuous monitoring of user behavior habits. The main problem with this method is that it is applicable only to certain applications. In our research work, we use the ML model with user behavior to improve dataset and accuracy. Unsupervised learning algorithms are mostly tried for internal threat detection in existing systems. This technique is easy because it does not require labeled or trained datasets. This algorithm directly uses unlabeled data to find abnormalities in user behavior patterns. The main significance pattern in this learning model is that it does not require training before the examination. This algorithm tends to detect irregular patterns in high-dimensional data automatically without human intervention. Threat detection using a graph is proposed using the unsupervised strategy of [14,15]. This technique keeps the data statically and checks the abnormality in the normal host nodes. Once the threat is detected, an unsupervised classifier is used dynamically for mining accurate threats [16].

III. Proposed System

The data sources in the cloud are valuable information that can be steeled by attackers because cloud security is a major issue. The security of the cloud network is already secured, although internal

attackers still exist. Those internal/insider attackers obtain access to valuable information in the system. The information leakage from the cloud server through an insider is a major issue that leads to the loss of data. In the current research, ML algorithms are used widely for cloud security. ML algorithms with behavioral analysis will help detect and predict insider threats, such as employees and contractors. In this study, to detect insider threats, the combination of interaction behavioral characteristics of the insiders, such as keystroke and mouse dynamics, which are considered for feature extraction and deep learning algorithm called deep belief network (DBN), has been used to predict the abnormal behavior of the insiders in the cloud network.

Insider threats pertain to the security threats caused by people in the organization called employees. These illegitimate accesses of the information may negatively affect the organization's policies and leads to loss of data. These attackers are categorized into two types: traitors and masqueraders. The former are a familiar person who knows the information and assets of the organization, and their behavior fulfills the security policies of the organization. In comparison, the latter are the attackers who gain illegal access to the identity of legitimate users. Moreover, traitors have more information about the access policies, data storage location, and intellectual property details than masqueraders. In this study, the cruel insider from the organization is identified by monitoring their interaction behavior. They are working with their corresponding duties, but their activities are not normal. Based on their actions, the normal users are identified as malicious users. The interaction of the user is categorized into two, namely, rich keystroke and rich mouse operations. With these two kinds of operations, the user can interact with all kinds of data and applications in the cloud system. We assume that these two interaction operations range [0, 1]. The 0 value means key operations, whereas 1 means mouse operations

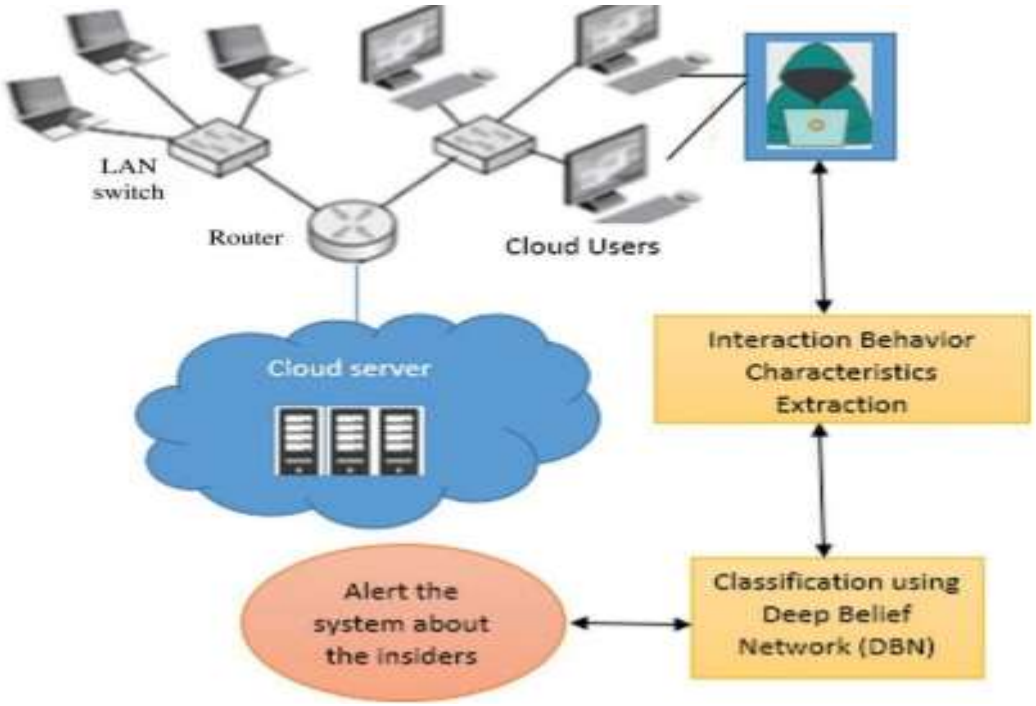

Fig 1: Overview of Proposed System

IV. Evaluation

Following the prediction phase, we must use various evaluation metrics to assess the correctness of the model results, such as accuracy, precision, recall, and F1 − Score. The accuracy metric is a type of evaluation statistic that evaluates how accurate a classifier is. We simply add up the samples that were correctly predicted (true positive and true negative) and divide that amount by the number of samples to determine the accuracy using the confusion matrix; see Equation (1). In our case, we will classify the data into two categories: normal and abnormal, and the accuracy metric will give the percentage

of the user's activities that are classified correctly.

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

where:

TP: predicted abnormal activity is an abnormal activity;
FP: predicted normal activity is an abnormal activity;
FN: predicted abnormal activity is a normal activity;
TN: predicted normal activity is a normal activity.

We can use these elements as input to calculate additional evaluation metrics, as demonstrated in Equation (2). Precision is a measurement of precision that provides us with a measure of exactness, which determines the number of all true predictions of anomaly (or abnormal activity) on all predictions. We can obtain 100% accurate predictions if the precision value is close to 1, which indicates that FP≈0FP≈0. There were four distinct classification models that we utilised. Compared to the anomaly detection methods, the ML classification models produced the best overall results. The SVM model achieved the best results by successfully identifying all threat users.

The primary step in the SVM experiment is finding the best combination of C and gamma parameters. A high value of C attempts to minimise the misclassification of the training data, while a low value smooths the model. Conversely, if the gamma value is too large, it will lead to an overfitting problem. As the findings show, relying on SMOTE to achieve an equal balance with the majority class may not always the best option, depending on the desired outcome. Despite the fact that SMOTE did not raise the F1 − Score in the NN model, it boosted recall at the expense of accuracy and precision, an entirely desirable outcome when it comes to detecting insider threats, as a few false alarms are more desirable than undetected attacks.

We would also like to emphasise that the original SMOTE paper [52] achieved excellent results by combining SMOTE and random under-sampling. Under-sampling was not used in this study because all data instances were necessary. Random forest and AdaBoost are machine learning algorithms designed explicitly for imbalanced datasets. We note that SMOTE is not required to achieve excellent results with these two methods. The overall performance of AdaBoost is superior to that of the random forest in all cases.The main similarity is that they handle collecting the data the same way as this research, where each data instance represents a user feature vector. The SVM model obtained the highest overall performance compared to the other algorithms. It achieved 100% accuracy. Furthermore, it has a higher recall (100%) and fewer false alarms. Additionally, the CNN model [34] has achieved a high accuracy (100%). However, since no values are provided for the other evaluation metrics, it is difficult to ascertain how well they are doing.

V. Conclusion

This article tends to achieve high performance in insider attack detection. Internal attackers always seem to be very intelligent to hide as an attacker and work as a trusted authority. IT makes every communication possible via networks with high-speed digital processing techniques. When the world is very happy to establish and use digital communications, others are unhappy because of insider attackers of sensitive and confidential data in the networks. In our article, we introduce the user interaction behavior pattern with a deep belief neural network. The behavior of the user is recognized through detecting mouse movements and clicks and keystrokes in their system and is collected for the training layer in DBN. This study shows the results based on trained pattern unauthorized entry. The accuracy of the proposed model is improved when compared with that of SVM and LSTM. DBN is an ML model, which acts like a neuron based on available knowledge and produces 99% outperforming results. In future studies, the ensemble deep learning models can be used for detecting the internal attacks in most sensitive applications, such as the military, hospitals, and banking. An ensemble method proves its efficiency and performance in many applications.

References

1. Homoliak, F. Tofalini, J. D. Guarnizo, Y. Elovici and M. Ochoa, “Insight into insiders: A survey of insider threat taxonomies, analysis, modeling, and countermeasures,” ACM Computing Surveys, vol. 52, no. 2, pp. 1–40, 2019.
2. M. N. Al-Mhiqani, R. Ahmad, Z. Z. Abidin, W. M. Yassin, A. Hassan et al., “A new taxonomy of insider threats: An initial step in understanding authorised attack,” Information System Management, vol. 1, pp. 343–359, 2018.
3. J. Kim, M. Park, H. Kim, S. Cho and P. Kang, “Insider threat detection based on user behavior modeling and anomaly detection algorithms,” Applied Sciences, vol. 9, no. 19, pp. 1–21, 2019.
4. T. Qiu, H. Wang, K. Li, H. Sheng, A. Sangaiah et al.,"A novel machine learning algorithm for spammer identification in industrial mobile cloud computing,” IEEE Transaction on Industrial Informatics, vol. 15, no. 4, pp. 2349–2359, 2015.
5. N. Nguyen, P. Reiher and G. H. Kuenning, “Detecting insider threats by monitoring system call activity,” in Proc. ISW, West Point, NY, USA, pp. 45–52, 2003.
6. R. V. Yampolskiy and V. Govindaraju, “Behavioural biometrics: A survey and classification,” International Journal of Biometrics, vol. 1, no. 1, pp. 81–113, 2008.
7. F. Monrose, M. K. Reiter and S. Wetzel, “Password hardening based on keystroke dynamics,” International Journal of Information Security, vol. 1, no. 2, pp. 69–83, 2002.
8. K. S. Killourhy and R. A. Maxion, “Comparing anomaly-detection algorithms for keystroke dynamics,” in Proc. DSN, Lisbon, Portugal, pp. 125–134, 2009.
9. CENELEC-EN 50133-1, “Alarm systems. access control systems for use in security applications. part 1:System requirements,” Belgium, 1996. [Online]. Available: https://standards.globalspec.com/std/390063/EN%2050133- 1.
10. Y. Liao and V. R. Vemuri, “Using text categorization techniques for intrusion detection,” in Proc. USENIX Security Symposium, vol. 12, pp. 51–59, 2002.
11. D. Y. Yeung and Y. Ding, “Host-based intrusion detection using dynamic and static behavioral models,” Pattern Recognition, vol. 36, no. 1, pp. 229–243, 2003.
12. S. Mathew, M. Petropoulos, H. Q. Ngo and S. Upadhyaya, “A datacentric approach to insider attack detection in database systems,” in Proc. RAID, Ottawa, Ontario, Canada, pp. 382– 401, 2010.
13. D. J. Cook and L. B. Holder, “M Ining Graph Data,” Hoboken, NJ, United States: John Wiley & Sons, 1st Edition. 2006.
14. W. Eberle and L. Holder, “Discovering structural anomalies in graph-based data,” in Proc. ICDM, Omaha, NE,USA, pp. 393–398, 2007.
15. M. M. Masud, Q. Chen, L. Khan, C. Aggarwal, J. Gao et al., “Addressing concept-evolution in concept-drifting data streams,” in Proc. ICDM, Sydney, NSW, Australia, pp. 929–934, 2010.
16. X. Wang, Q. Tan, J. Shi, S. Su and M. Wang, “Insider threat detection using characterizing user Industrial Engineering Journal ISSN: 0970-2555 Volume : 51, Issue 03, March : 2022 UGC CARE Group-1, 246 behavior,” in Proc. DSC, Guangzhou, China, pp. 476–482, 2018.
17. X. Chen, J. Shi, R. Xu, S. M. Yiu, B. Fang et al., “PAITS: Detecting masquerader via shortlived interventionalmouse dynamics,” in Proc. ATIS, Melbourne, VIC, Australia, pp. 231– 242, 2014.
18. J. R. Schoenher and R. Thomson, “Insider threat detection: a solution in search of a problem,” in Proc. Cyber Security, Dubin, Ireland, pp. 1–7, 2020.
19. L. Nkosi, P. Tarwireyi and M. O. Adigun, “Insider threat detection model for the cloud,” in Proc. Is, South Africa, pp. 1–8, 2013.
20. C. Xiaojun, W. Zicheng, P. Yiguo and S. A. Jinqiao, “Continuous re-authentication approach using ensemble learning, Procedia Computer Science, vol. 17, pp. 870–878, 2013.
21. B. Gabrielson, “Who really did it? Controlling malicious insiders by merging biometric behavior with detectionand automated responses,” in Proc. SS, Maui, HI, USA, pp. 2441– 2449, 2012.

22. Y. Park, I. M. Molloy, S. N. Chari, Z. Xu, C. Gates et al., "Learning from others: user anomaly detection using anomalous samples from other users. in Proc. ESORICS, Vienna, Austria, pp. 396–414, 2015.
23. N. Kanaskar, J. Bian, R. Seker, M. Nijim and N. Yilmazer, "Dynamical system approach to insider threat detection," in Proc. ISC, Boston, MA, USA, pp. 232–238, 2011.
24. P. Parveen, N. McDaniel, V. S. Hariharan, B. Thuraisingham and L. Khan, "Unsupervised ensemble-based learning for insider threat detection," in Proc. PSRT, Amsterdam, The Netherlands, pp. 718–727, 2012.
25. F. Y. Leu, K. L. Tsai, Y. T. Hsiao and C. T. Yang, "An internal intrusion detection and protection system by using data mining and forensic techniques. IEEE Systems, vol. 11, pp. 427–438, 2017.