Review on Insider Threat Detection Techniques

T. O. Oladimeji¹, C. K Ayo¹ and S.E Adewumi¹,²
1. Department of Computer & Information Sciences, Covenant University, Ota, Lagos
2. Department of Computer Science, Federal University Lokoja, Kogi State

Abstract: An insider, also regarded as an employee of a company, becomes a threat when the intention or action can affect the company negatively. Insider threat has been an eminent problem in organizations that has resulted in the loss of trust, confidential data and information. This study seeks to review current existing techniques to insider threat detection and also proffers machine learning technique as the way forward for insider threat detection.

1. Introduction

An ‘insider’ is any individual who is currently working or has worked for an organization and has access to its information technology (IT) infrastructure [1]. There are two main classifications of an insider; malicious and non-malicious insider. A malicious insider is one that deliberately jeopardizes the operation of the company; it can therefore be considered an insider threat. A non-malicious insider on the other hand is an unintentional threat due to negligence or carelessness in the art of performing normal day-to-day role. It has been identified as one of the largest undetected threat to secured data [2].

Threat is someone or an action that has adverse effect on an organization’s asset. It includes but not limited to espionage, modification or theft of confidential data for personal gain, threat of customers’ information for a competing organization, sabotage, physical harm to company’s properties among others [3].

An insider threat is a present or previous worker, contract staff or business associates who has or had privileges to access the organization's network, system, or data and deliberately perform actions that will negatively affect the confidentiality, integrity, or availability of the organization's information or information systems [4]. It has been considered the most dangerous kind of threat to any organization [5].

Insider threat is still seen as the major security issue for organizations and was reported as the major security concern in organizations [6]. Amongst 874 cases documented in a report [5], 191 cases were caused by malicious employees, 568 cases were attributed to negligence of staff and only 85 cases by masqueraders. These eye-opening statistics implies that 759 cases (approximately 87%) out of the 874, were caused by internal threat. More than 70% of the companies used in the survey affirmed that they were susceptible to insider threat. Several times, insider threat cases are not reported, due to ethical laws and sanctions issued out by the government.
2 Insider Threat Detection Techniques

In this section, the insider threat detection techniques, will be discussed under two major subsections: machine and non-machine learning techniques. Papers addressing each type will be reviewed.

2.1 Non-Machine Learning Techniques

In this section, non-machine learning approaches to insider threat detection will be discussed. Authors under this section introduced methods such as access control measures, block chain technology, tableau platforms amongst others.

Meng et al.[7] proposes the use of block chain to improve the performance of Intrusion Detection Systems (IDS). The authors claimed that the block chain technology was able to handle some unresolved challenges relating to IDS like: Overhead traffic with limited handling capacity, limited signature coverage, inaccurate profile establishment, massive false alerts & lack of review. A major drawback of the system is the high rate of false positives. High false rates are a big limitation for the anomaly-based detection. Block chain has not been used extensively in IDS despite its strength particularly in the area of data sharing and trust computation.

Liu et al.[8] highlighted three classification of insider threats as 1) data exfiltration, 2) integrity or availability violations and 3) sabotage of ICT systems. The authors believed that audit data source is highly important no matter the analytical technique adopted in an intrusion detection system. Host and network-based equipment are the major sources of data used in anomaly based intrusion detection systems. Examples of host-based data sources include system calls, Unix shell commands, keyboard and mouse dynamics, and other system host logs. Network traffic and logs are examples of a network-based data source where information can be collected for network behavior modelling of any users, hosts, IP addresses, TCP flows and so forth. There is another rarely mentioned data source; contextual data source which contains employees psychological and human resource related information.

Ring et al.[9] developed a framework known as Coburg Utility Framework (CUF). It uses network data streams especially flows based data (consisting of Source IP Address, Source Port, Destination IP Address and Transport Protocol) from computers, switches or firewalls. The idea of using flow data instead of packet-based data was to reduce privacy and ethical issues relating to data usage.

Legg [10] tried overcoming the biggest challenge of insider threat; validating the developed system in a real organization using real life data. The organization provided 750,000 entries per day, but only 44,000 entries were authentic and therefore used. The system was deployed for a duration of 31 days over two different times. Although it generated quite a number of false positives, the author explained that it was due to the number of high alerts generated by individuals per day. The system was able to identify an employee, who was already on the watchlist of the company as a threat. This was therefore taken as a good sign that the system has potential for correctness. The ability of the machine to detect insider threat is largely dependent
on the training data set. It has been proven to reduce the search space of an occurrence, but it cannot totally replace a human analyst. The system also incorporated a visual analytic dashboard with four (4) views: User Selection, Projection, Detail and Feature.

Legg et al.[11] listed some requirements for developing an insider threat detection system. They include: the system should be able to 1. Give a score to each user determined by the level of threat posed. 2. Handle all categories of insider threat like sabotage, intellectual theft, fraud and so on. 3. Deal with previously unknown threat if it is classified as an anomaly for the user and role. 4. Compare the current and previous behaviors of users in that role and measure deviation.

Garae and Ko[12] used Tableau and Limkurious platforms to provide visualization to aid decision making process by the analyst. It not only helps to analyse the data, but also visually explain the steps taken to the attack occurrence. They thereafter proposed SCeeL-VisT as a security visualization standard that can be adapted by all organizations.

Sanzgiri and Dasgupta[13] discussed extensively on insider threat detection techniques under subheads like anomaly based approaches, Role based Access control, Scenario based, decoys and honeypots, risk analysis using psychological factors, Risk analysis using workflow, improve network defense, improve defense via access control and process control to dissuade insiders. Their work throw more light to the research domain.

2.2 Machine Learning Techniques

This section simplifies the techniques by classifying them into two sets: the classification and clustering machine learning techniques

2.2.1 Classification Machine Learning Techniques

Li et al. [14] introduced intrusion sensitivity to collaborative intrusion detection system. The collaboration was proposed to help IDS collect and learn experience from each other. It used K-Nearest Neighbor (KNN), as a supervised machine learning algorithm to automatically assign values of intrusion sensitivity to the Collaborative Intrusion Detection Networks (CIDNs). They integrated 200 alarms with three levels: high, medium and low. An initial experiment was done using KNN, Back-propagation Neural Network (BNN), and Decision Tree (DT). It was discovered that KNN performed better and was therefore used as the classifier for the experiment.

Sarma et al.[15] used KNN (K Nearest Neighbor) to classify the users into 4 groups: legitimate, possibly legitimate, possibly not legitimate and not legitimate groups. If the user is not within the legitimate group, the user is passed through the facial recognition module as a second level of authentication when the KNN classifies it outside legitimate.

Ronao and Cho[16] tried to address security issues with relational databases. There are very few IDS that address security in Relational Database Management System (RDBMS). The paper addresses role intrusions against a database operating access control model based on roles of the users. They built a normal behavior profile for each role and then detect anomalous behavior for
deviations. Random Forest (RF) was used for role recognition because of its identified strength of minimizing false-positives and false-negatives. For the feature selection process, PCA (Principal Component Analysis) was used. A total of 21 features were taken. The TPC-E database was used to as a simulation for a typical online transaction process workload of a brokerage firm.

Hamid et al.[17] used weka machine learning platform to classify the KDD CUP 1999 dataset for 17 Kstar, IBK, MLP, classification algorithm which include NaiveBayes, j48, DT, CR, Zeroramongst others. It concluded that to get the best of machine learning algorithm, there would be a need to do away with some feature which are not so important. This leads to feature extraction of important features.

2.2.2 Clustering Machine Learning Techniques

Zhang et al.[18] used Deep Belief Net (DBN) unsupervised learning technique to learn the behaviors of insiders and therefore detect insider threat. Four (4) stages were used in the model: log collection, log preprocessing which transforms the data into the standard numerical form, deep learning of insider behavior features and then log classification. They integrated and normalized the behavior logs using 1\N code discretization method, used Restricted Boltzmann Machine (RBM) iterations. The further works as stated by the authors are to improve the classification method, increase the detection rate, and train massive data in combination with big data technology to realize a better deep learning network model. Malicious insiders within an organization can be insignificant, but their effect on the organization can be disastrous.

Tiwari and Shrivastava[19] worked on the weakness of k-mean algorithm (the need for the number of clusters to be known before training commences) by introducing hill climbing algorithm, whose strength is finding a local optimum which can then be used to determine the number of clusters that will be used by the KNN algorithm. The only major observation raised by the authors is that the execution efficiency of the two algorithms has not been tested.

Al tabash and Happa[2] used Gaussian Mixture Model (GMM), to model the normal behavior of the insiders. Mixture Model is a derivation from Latent Variable Models, for modelling complex probability distributions. It used the shared probability to cluster observations modelling it as a linear combination. clusters observations based on their shared probability distribution.

Choras and Kozik[20] used deep and recurrent neural network model as an unsupervised approach to detect abnormal network activities in a system logs in real time. The focus was to develop an approach that can efficiently utilize the high velocity, heterogeneous streams of dataset and automate result generation that will require little human resource.

Lo et al.[21] hypothesizes that insider threat activity is non-deterministic, and prior learning most time does not lead to increased accuracy. They implemented the Damerau-Levenshtein DL, Jaccard and Cosine Distance. They also implemented Hidden Markov Model (HMM), in order to compare it with the three distances mentioned above. The work showed that the three distance metrics, did not perform to the standard of HMM, but it was reported faster due to the low complexity of the algorithms.
Moustafa et al.[22] used the Dirichlet Multinomial Mixtures (DMM) model to develop an anomaly detection system. This is a type of the mixture model, which has been found to be very effective in detecting outliers or anomalies. Other mixture models include Gaussian Mixture Models (GMM), Beta Mixture Model (BMM). Of these three types of Mixture Models, this study claims that DMM does a better job of fitting and boundary definition of data because it is made up of a set of probability distributions.

Tuor et al [23] used Deep Neural Network (DNN) to detect anomaly from large stream of network logs in real time. The raw system logs were entered into the feature extractor with one vector per day as resulting output for each user. These vectors are then fed into a neural network, which creates a network per user. These networks are used to predict the next vector for each user, by first learning the normal behavior of each user and then predict anomaly using the Long Short-Term Memory (LSTM) form of the Recurrent Neural Network. The developed model was then compared with one-class SVM, PCA and isolation forest for accuracy and performance test, using scikit-learn and was reported to perform better than the techniques it was compared with.

Meryem et al.[24] tried to detect intrusion using map reduction and NSLKDD database. The authors first centralized all the log files into a matrix by mapping each log line into a row matrix, before assigning a weight (dependent on the number of occurrence) to each event using MapReduce Programming. After this, unlabeled behaviors were classified using K-means algorithm. KNN algorithm was applied on NSLKDD training set to be used to classify labeled attacks. The work developed a misuse detection system, which implied that the system has a database of all known attack, it then compares a new attack with the database. This system can be very effective for an attack that is previously known. They used python, sci-kit library on the HDFS Hadoop architecture were used for implementation. They made use of the NSLKDD data which is an improvement over KDDCUP99, because the number of biased classifiers were drastically reduced.

Lin, Zhong, Jia and Chen[25] used a hybrid approach to detect insider threat. It used the unsupervised Deep Belief Network (DBN) to extract features of the log from several sources. Since DBN is a model built on multilayer Restricted Boltzmann Machine (RBM), then it applied a one-class SVM (OCSVM) on it to train the classifier for to classify a given unknown future dataset. The author used deep learning for feature learning because they discovered that other learning methods suffer from large information loss.

Legg et al.[11] presented a systematic approach for insider threat detection and analysis following the concept of anomaly detection. Taking as input a large record of activity logs, the detection systems builds a tree-like profile for each user and role. These profiles are then compared in other to know how deviated the current daily observation is from the previously observed activities. A feature set representation is then built to capture the observations for each day and to note the variations of the current day features from the previously observed days. Principal Component Analysis (PCA) was then used on these large feature set, to reduce it into multiple anomaly assessment scores.
Tuor et al.[26] made use of computer logs to guess the user roles. Recurrent Neural Networks (RNN) was then used to refine the predictions. It was reported that RNN reduced the false positive ratio by about 30%. As further work, there is need to discover richer features that can improve the user role classification. There is also a need to introduce resampling methods in an attempt to balance the data, since most insider threat have very few identified threat, which can naturally lead to bias results.

Ahmed, Mahmood and Islam[27] gave an insightful, easy to read and comprehensive viewpoint to clustering unsupervised techniques for financial fraud detection. It explained extensively on the use of k-means algorithm as a partitional clustering algorithm.

3. Discussion

Stemming from the literature review in section 2, machine learning algorithm have a higher chance of positive result for research work in insider threat detection. This is because of its advantages like: wide area of application, can work on diverse kind of data with several dimensions, it utilizes resources efficiently, it can be used to automate repetitive tasks with the same quality of output as humans [20].

4. Conclusion

Insider threat is a major issue to all corporation. Designing an effective mitigation strategy to combat the problem has been a reoccurring research problem. Machine learning techniques have been proffered as a solution to similar issues like Anomaly Detection (AD), Network Intrusion Detection (NID) amongst others. This paper has done a review of non-machine learning and machine learning techniques for insider threat detection and concluded that machine learning technique is a promising solution for insider threat detection.

5. Acknowledgement

The authors do express their gratitude to the Management of Covenant University and to the University's Research Centre (CUCRID), Ota, Nigeria for sponsoring the publication of this article.

6. References

[1] G. B. Magklaras and S. M. Furnell, "A preliminary model of end user sophistication for insider threat prediction in IT systems," Computers & Security, pp. 371-380, 2005.

[2] K. Al tabash and J. Happa, "Insider - threat Detection using Gaussian Mixture Models and Sensitivity Profiles," Computer & Security, pp. 1-22, 2018.

[3] B. Balakkrishman, "Insider Threat Mitigation Guidance," The SANS Institute, 2015.

[4] "CERT," 2014. [Online]. Available: https://www.cert.org/insider-threat/.
[5] D. Costa, "CERT definition of 'Insider Threat','" 7 March 2017. [Online]. Available: https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html.

[6] M. Gogan, "Insider Threats as the main Security Threat in 2017," 11 April 2017. [Online]. Available: https://www.tripwire.com/state-of-security/security-data-protection/insider-threats-main-security-threat-2017/.

[7] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang and J. Han, "When Intrusion Detection Meets Blockchain Technology: A Review," SPECIAL SECTION ON RESEARCH CHALLENGES AND OPPORTUNITIES IN SECURITY, pp. 10179 - 10188, 2018.

[8] L. Liu, O. D. Vel, Q.-L. Han, J. Zhang and Y. Xiang, "Detecting and Preventing Cyber Insider Threats: A Survey," IEEE COMMUNICATIONS SURVEY & TUTORIALS, pp. 1-21, 2018.

[9] M. Ring, S. Wunderlich, D. Grudl, D. Landes and A. Hotho, "A Toolset for Intrusion and Insider Threat Detection," Data Analytics and Decision Support for Cybersecurity, pp. 17-31, April 2017.

[10] P. A. Legg, "Human-Machine Decision Support Systems for Insider Threat Detection," Data Analytics and Decision Support for Cybersecurity, pp. 46-66, April 2017.

[11] P. A. Legg, O. Buckley, M. Goldsmith and S. Creese, "Automated Insider Threat Detection System using User and Role-based Profile Assessment," IEEE SYSTEMS JOURNAL, pp. 503 - 512, 2017.

[12] J. Garae and R. K. Ko, "Visualization and Data Provenance Trends in Decision Support for Cybersecurity," Data Analytics and Decision Support for Cybersecurity, pp. 251 - 275, April 2017.

[13] A. Sanzgiri and D. Dasgupta, "Classification of Insider Threat Detection Techniques," in CISRC '16 Proceedings of the 11th Annual Cyber and Information Security Research Conference, New York, USA, 2016.

[14] W. Li, W. Meng, L.-F. Kwok and H. H. IP, "Enhancing Collaborative Intrusion Detection Networks against Inside Attacks using Supervised Intrusion Sensitivity-Based Trust Management Model," Network and Computer Applications, pp. 135-145, 2017.

[15] S. M. Sarma, Y. Srinivas, V. M. Abhiram, L. Ullala, M. S. Prasanthi and J. R. Rao, "Insider Threat Detection with Face Recognition and KNN User Classification," in International Conference on Cloud Computing in Emerging Markets (CCEM), Bangalore, India, 2017.

[16] C. A. Ronao and S.-B. Cho, "Anomalous Query Access Detection in RBAC-administered Databases with Random Forest and PCA," Information Sciences, pp. 238-250, 2016.
[17] Y. Hamid, M. Sugumaran and L. Journaux, "Machine Learning Techniques for Intrusion Detection: A Comparative Analysis," in *INTERNATIONAL CONFERENCE ON INFORMATICS AND Analytics (ICIA '16)*, Pondichery, India, 2016.

[18] J. Zhang, Y. Chen and A. Ju, "Insider threat detection of adaptive optimization DBN for behavior logs," *Turkish Journal of Electrical Engineering & Computer Sciences*, pp. 792-802, 2018.

[19] S. K. Tiwari and M. Shrivastava, "Implementation of Improved K-Mean Algorithm for Intrusion Detection System to Improve the Detection Rate," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, pp. 2456-3307, 2018.

[20] M. Choras and R. Kozik, "Machine Learning Techniques for Threat Modeling and Detection," *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks*, pp. 179-192, 2018.

[21] O. Lo, W. J. Buchanan, P. Griffiths and R. Macfarlane, "Distance Measurement Methods for Improved Insider Threat Detection," *Security and Communication Networks*, pp. 1-18, 2018.

[22] N. Moustafa, G. Creech and J. Slay, "Big Data Analytics for Intrusion Detection System: Statistical Decision-Making using Finite Dirichlet Mixture Models," *Data Analytics and Decision Support for Cybersecurity*, pp. 137-177, April 2017.

[23] A. Tuor, S. Kaplan, B. Hutchinson, N. Nichols and S. Robinson, "Deep Learning for Unsupervised Insider Threat Detection in Structured Cybersecurity Data Streams," pp. 1-9, 2017.

[24] A. Meryem, D. Samira, E. O. Bouabid and L. Mouad, "A Novel Approach in Detecting Intrusions Using NSLKDD Database and MapReduce Programming," in *the 14th International Conference on Mobile Systems and Pervasive Computing (MobiSPC2017)*, 2017.

[25] L. Lin, S. Zhong, C. Jia and K. Chen, "Insider Threat Detection Based on Deep Belief Network Feature Representation," in *2017 International Conference on Green Informatics*, 2017.

[26] A. Tuor, S. Kaplan, B. Hutchinson, N. Nichols and S. Robinson, "Predicting User Roles from Computer Logs Using Recurrent Neural Networks," in *Proceedings of the Thirty-First AAAI Conference on Artificial Intelligence (AAAI-17)*, 2017.

[27] M. Ahmed, A. N. Mahmood and M. R. Islam, "A Survey of Anomaly Detection Techniques in Financial Domain," *Future Generation Computer Systems*, pp. 278-288, 2016.
[28] P. Legg, "Visualizing the insider threat: Challenges and tools for identifying malicious user activity," in *IEEE Symposium on Visualization for Cyber Security*, Chicago, Illinois, USA, 2015.

[29] P. A. Legg, O. Buckley, M. Goldsmith and S. Creese, "Caught in the Act of an Insider Attack. Detection and Assessment of Insider Threat," in *IEEE International Symposium on Technologies for*, Waltham, USA, 2015.