Research Opportunity of Insider Threat Detection based on Machine Learning Methods

Noer Tjahja Moekthi Prajitno
Department of Information System, School of Postgraduate Studies
Diponegoro University
Semarang, Indonesia
noer@students.undip.ac.id

H. Hadiyanto
School of Postgraduate Studies, Diponegoro University
Semarang, Indonesia
hadiyanto@live.undip.ac.id

Adian Fatchur Rochim
Department of Computer Engineering, Faculty of Engineering
Diponegoro University
Semarang, Indonesia
adian@ce.undip.ac.id

***Abstract*— Insider threats have been a known threat since a long time ago in the information technology field and many researchers tried to create novel methods to solve this threat. The purpose of this paper is to find research opportunities for insider threat detection. This was done by finding and reviewing papers related to insider threat detection. The papers reviewed were only the ones that utilized machine learning algorithms because they were the most common method used by researchers to detect malicious insiders. A systematic literature review by Kitchenham, which consisted of planning, selection, extraction, and execution, was employed as the methodology. The detection method was classified into three categories: combination, selection, and singular focus. Each category discussed and recommended a research direction to create a potentially better solution for insider threat problems.**

Keywords— insider threat, machine learning, detection

I. INTRODUCTION

Insider threat has been one of the known cyber threats since a long time ago. The threat assumes access control or credential is on the hand of the malicious side. Armed with the authority, an insider can make critical damage to an organization's system. Attackers have long been known as one of the cyberspace threats. The threat assumes that attackers have had access or credential within the system and thus can perform all functions owned by an authorized account. The authorization owned by insider attackers can cause great damage to the organization. In addition, the advance of technology and users' skills in using the technology have made it difficult and also crucial to detect cyber attacks. According to a survey of 515 respondents conducted by CSO online in the USA in 2018, 25% of cyberspace attacks are insider threats [1]. Furthermore, the survey also reported that there is an increase in the average time needed to detect an intrusion or an attack on an organization's network, from 80.5 days in 2016, 92.2 days in 2017, to 108.9 days in 2018. This means that there is a 35% increase in time needed to detect intrusion in 2018. In 2022, Ponemon Institute reported that there is an increase of 44% in the number of insider threat incidents within the last 2 years [2]. The cost spent by organizations as a result of credential theft has also increased from $2.79 million in 2020 to $4.6 million in 2022, an increase of 65%. Based on those facts, research on solutions to insider threats is a significant security topic nowadays.

There have been many studies and literature reviews addressing the issue of insider threats for the last few years. Liu and the team conducted a comprehensive study on insider threats by distributing a survey in 2018 [3]. In the survey, they classified insider threats into 3 categories, namely, masquerader, traitor, and unintentional preparator. In 2021, Xiaoxiao Ma and partners conducted a survey related to a study on graph anomaly detection using Deep Learning [4]. In the same year, Shuhan Yuan and Xintao Wu wrote a literature review on insider threats and focused only on a detection method that is based on Deep Learning Technique [5]. In 2022, Montano and his partners did a research survey on insider threats [15]. This survey focused on solutions to one of the impacts of insider threats which is data leakage.

In this literature review, we focused on recent research that utilized machine learning to create an insider threat detection model. In section 2, we defined insider threat, a term that we used as the main keyword in searching papers that would be reviewed by us. In section 3, we showed paper results after employing the Kitchenham method and classified them into three main categories. Section 4 is the last part of our literature study. This section discussed our recommendation for future research addressing the solution to insider threat issues.

II. DEFINING INSIDER THREAT

A. Insider Threat

In general, an insider threat is defined as a threat from inside, or in other words, it can be assumed that all people who legitimately have access or privilege in an organization may become an insider threat to the organization [10]. In the survey conducted by Liu et.al, insider threats are divided into several types, namely, masquerader, traitor, and unintentional preparator [3]. Masqueraders can steal access and threaten a system from inside by employing many different illegal ways, such as social engineering, scam, phishing, sniffing, installing backdoors or malware leading to intrusion into the account or legitimate user credential, or compromised users. A compromised credential or an intrusion is called a compromised user credential, or CUC, which is used by Shah to define insider threats in his study [12]. In another study, a compromised user is also called a compromised account, which means the same as CUC [6]. An intrusion can occur not only to an account with a closed system in an organization but also to an online social network or OSN [13][14]. With different aims of use, the activity data of compromised users are usually different from the activities log of normal users or authorized users of the system. Data that has unusual or different patterns from normal use is called anomaly [8]. Apart from 'anomaly', there are several terms that have the same meaning as 'anomaly', such as 'unusual', 'irregular', 'rare', 'strange', 'novelty', and 'outlier' [19].

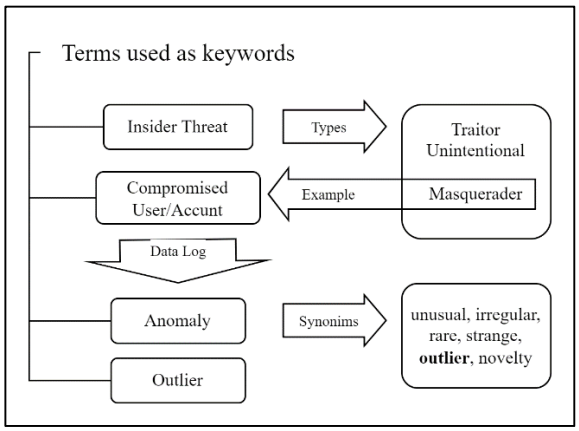

Fig. 1. Finding keywords to search literature

III. KITCHENHAM RESEARCH METHOD

To search and filter out the research papers we employed a method from Kitchenham [63]. The first step of the Kitchenham method is planning. We defined three research questions which were:

- RQ1: How to detect insider threats in an organization's information system?
- RQ2: How to utilize machine learning in the detection?
- RQ3: How to evaluate the detection method?

The second step is selection. We searched papers using 'insider threat' and its related terms such as 'compromised user or account', 'anomaly', and 'outlier' as the keywords using search tools such as Scopus and Google Scholar. We searched papers that were published after 2018, had citations, and were published in trustworthy journals. The process of how we found those related keywords was represented in Figure 1. At first, as many as 901 papers were found, and then we filtered and picked 63 of them. After that, we did a quick read to find relevant papers to RQs, and 53 papers were left.

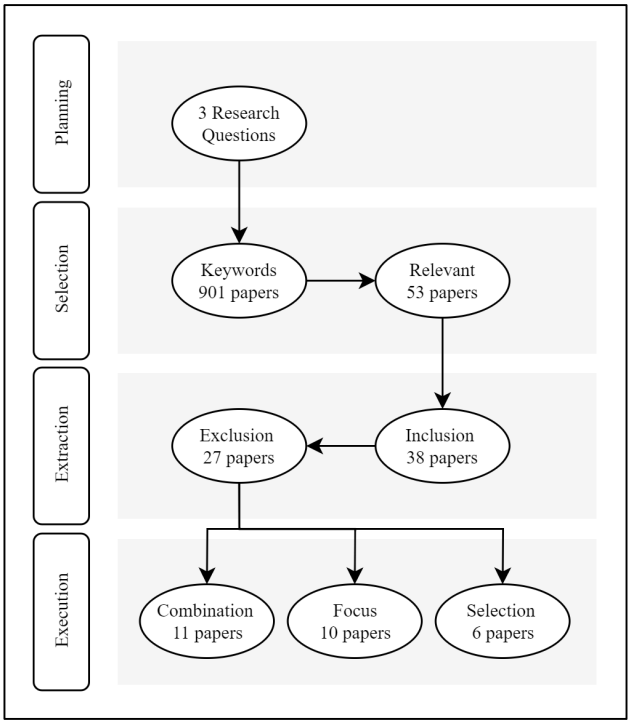

Fig. 2. Implementing Kitchenham Method

The third step is extraction which is separated into inclusion and exclusion. We included only papers that proposed a detection model to detect insider threats. After inclusion, the remaining papers were 38. Furthermore, we excluded papers with no machine learning algorithm in suggesting the detection method and there were 27 papers left.

The last step is extraction. We categorized the 27 papers into three categories based on how the researcher utilized machine learning algorithms. The categories were combination, focus, and selection. The combination category had the most papers which were 11, the focus category had 10 papers and the remaining 6 were in the selection category. The whole implementation of the Kitchenham method was represented in Figure 2.

A. Combination

The Combination category consists of papers that utilize multiple machine learning algorithms, combining them to produce better detection performance. In addition, the algorithms could be used separately in different circumstances but later combined in the evaluation. The combination category also could be called hybrid learning. According to our review in Table I, Auto Encoder, LSTM, and Neural Networks were the most used machine learning algorithms to be combined with other techniques.

TABLE I. COMBINATION CATEGORY PAPERS

Ref	Algorithm	Dataset	Evaluation
[30]	Gated Recurrent Unit, skipgram	Enron Email, Twitter	Acc.
[50]	Auto Encoder, Isolation Forest, LODA, Local Outlier Factor	CERT r4.2, CERT r6.2	AUC
[51]	LR, RF, ANN, NB, AE, PCA, RP	CERT r4.2, CERT r5.2	Acc., Prec., AUC, Recall
[13]	NLP-Word Embedding, KNN	NSL-KDD	Prec., Recall
[46]	Linear Manifold learning, GAN	CERT r4.2, CERT r5.2	Prec., Recall, FScore, Kappa, MCC
[49]	Locally Aware Patch Feature, Nearest Neighbor Search, Gaussian	MVTec	AUC
[41]	One-Class Adversarial Nets, LSTM, GAN	UMDWiki.	Acc., AUC, Recall, FScore
[55]	C-GAN, MLP, 1DCNN, RF, XGBoost	CERT r4.2	Prec., Recall, FScore, Kappa, MCC
[62]	LSTM-Autoencoder	CERT r4.2	Acc., Prec. , FScore
[39]	Temporal Point Processes, Recurrent Neural Networks	CERT r6.2, UMDWiki.	AUC
[33]	Cascaded Autoencoders, Bidirectional LSTM	CERT r6.2	AUC, Recall

B. Focus

The focus category contains papers that have one main machine learning algorithm to detect insider threats. The algorithm could be based on an existing technique that has further improvement by the researcher or combined with a non-machine learning algorithm. It also could be a novel

learning technique inspired by other algorithms. The focus papers were shown in Table II.

TABLE II. FOCUS CATEGORY PAPERS

Ref	Algorithm	Dataset	Evaluation
[58]	Deep Belief Neural Network, Restricted Boltzmann Machine	Cooja Simulator	Acc., FScore
[53]	NB, Max. Likelihood Estimate, Max. A-Posteriori, Expectation-Max.	CERT r4.1	AUC
[18]	Self-Supervised Deep Representations, One-Class Classifier	MVTec	AUC
[45]	Memory-Augmented Autoencoder (MAA), Temporal-Spatial Fusion	CERT r6.2	AUC
[60]	Deep Metric Neural Network, Monte Carlo Sampling	TPC-E	Acc., Prec., Recall, FScore
[36]	Bidirectional Encoder Representations from Transformers	BGL, HDFS, TBird, UCI	Prec., Recall, FScore
[24]	Gradient boosting machines (GBM)	Balabit	AUC, EER
[37]	Dirichlet Marked Hawkes Process	CERT r?, UMDWiki.	AUC
[38]	Self-Supervised Pre Training, Metric based Few-Shot Learning,	CERT r?, UMDWiki.	Prec. Recall, FScore
[59]	BiLSTM, Sliding Window Algorithm	Testbed	Acc., FNR

C. Selection

Similar to the combination category, the selection category includes papers that have multiple machine learning algorithms for detecting insiders. The main difference is that rather than being combined, the machine learning algorithms are compared to each other and the one that has the best performance is selected. Based on our review in Table III, most papers used conventional machine learning techniques and the novelty of the papers was shown in how the researchers selected the best technique.

TABLE III. SELECTION CATEGORY PAPERS

Ref	Algorithm	Dataset	Evaluation
[34]	SVM, RF	CERT r?	Acc.
[21]	NB, LR, RF, SVM, KNN, DT, LSTM, GRU	CERT r4.2	Acc., Prec., AUC, Recall, FScore, TNR., FNR
[29]	LR, RF, ANN	CERT r5.2	Prec., Recall
[17]	Gauss, Parzen, PCA, KMC (K=3,5,10), Parzen+PCA	CERT r6.2	Recall
[52]	LSTM, NN, RF, XGBoost, SVM	Contiki Simulator	Acc., Prec., Recall, FScore
[6]	NLP, XGBoost, Multi-Criteria Decision Making, ANP	Twitter	Acc., FScore

IV. SUMMARY AND RECOMMENDATION

This study grouped studies on machine learning-based insider threat detection into combination, focus, and selection. According to the literature that we have reviewed, the recommendation of the study, research opportunity, and research challenges are divided into 2 points.

A. Detection: Combination and Selection Learning

A study on the improvement of insider threat detection performance has been proven to have a good result by using some machine learning algorithms simultaneously [17][29][51] or by choosing based on the weight of the performance with the help of expert system so that machine learning can adjust the best performance according to the dataset used [21]. The stages of the process commonly start with data processing, feature selection, data learning, detection, and evaluation [6][62]. Combining methods from the beginning of the process to the final process can be further tested considering that the methods which have not been tried are still many. In addition, machine learning methods that were in the focus category can be used as one of the combined or selected algorithms. The combination of learning methods could generate a novel method that may have a better performance, particularly in some types of datasets. Research challenges to improve the performance lies in the previous high performance which, in some cases, has recall, accuracy, AUC, and precision up to 99% or more [21][51][53][49][29][38].

B. Fairer Evaluation Model

In evaluating the performance of insider threat detection, recall, accuracy, AUC, FScore, and precision were often used. However, those evaluation results still cannot be considered the same as the real case performance. This occurs because in the dataset tested there are very few malicious activities of insiders. For example, in the use of accuracy evaluation in CERT 6.2, there are a total of 135,117,169 activities data, but there are only 470 malicious activities [5]. If a trial on detection of the whole dataset is performed and arbitrarily all tests are considered as non-insiders or “normal”, the accuracy performance achieved will be more than 99.9%. In addition, the characteristics of static or fixed datasets are the opposite of the condition in real life where the datasets constantly change over time with data logs added dynamically and indefinitely. This can result in performance discrepancy between research and implementation as Erola et.al. conducted [9]. In the study by Erola et.al., the detection method cannot be implemented properly in three organizations that have different conditions. The use of real data in an organization can help to represent the circumstance of a performance trial better, However, the main concern is private or confidential data, thus it is difficult to prove or compare the research result with other methods or even to be developed further by the other researchers. An example of this case is a study by Saleh which claimed to be 100% accurate in detecting CUC [12]. The researchers did not openly disclose the dataset they used due to confidentiality. As a result, it is difficult for other researchers to verify the claims or even further improve the method. Based on those problems, it can be said that it is necessary to develop a fairer evaluation model which takes into account not only TP, TF, NP, and NF, but also other variables such as data availability and time.

For further research, reviewing insider threat literature that was filtered out is recommended. More classification could be achieved outside detection, such as review and evaluation. With a broadened view, more research opportunities on insider threat topics could be found.

REFERENCES

[1] M. Nadeau, "State of cybercrime 2018: Security spending up, but so are the risks," CSO Online, Nov. 02, 2018. https://www.csoonline.com/article/3318496/state-of-cybercrime-2018-security-spending-up-but-so-are-the-risks.html (accessed Oct. 20, 2022).

[2] Ponemon Institute, "2022 Ponemon Cost of Insider Threats Global Report," Proofpoint, 2022. https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats (accessed Oct. 20, 2022).

[3] L. Liu, O. De Vel, Q.-L. Han, J. Zhang, and Y. Xiang, "Detecting and Preventing Cyber Insider Threats: A Survey," IEEE Communications Surveys & Tutorials, vol. 20, no. 2, pp. 1397–1417, 2018, doi: 10.1109/comst.2018.2800740.

[4] X. Ma et al., "A Comprehensive Survey on Graph Anomaly Detection with Deep Learning," IEEE Transactions on Knowledge and Data Engineering, pp. 1–1, 2021, doi: 10.1109/tkde.2021.3118815.

[5] S. Yuan and X. Wu, "Deep learning for insider threat detection: Review, challenges and opportunities," Computers & Security, vol. 104, p. 102221, May 2021, doi: 10.1016/j.cose.2021.102221.

[6] S. Alterkavı and H. Erbay, "Novel authorship verification model for social media accounts compromised by a human," Multimedia Tools and Applications, vol. 80, no. 9, pp. 13575–13591, Jan. 2021, doi: 10.1007/s11042-020-10361-2.

[7] J. Singh, A. Sinha, P. Goli, V. Subramanian, S. K. Shukla, and O. P. Vyas, "Insider attack mitigation in a smart metering infrastructure using reputation score and blockchain technology," International Journal of Information Security, vol. 21, no. 3, pp. 527–546, Sep. 2021, doi: 10.1007/s10207-021-00561-8.

[8] Y. M. Tukur, D. Thakker, and I. Awan, "Edge - based blockchain enabled anomaly detection for insider attack prevention in Internet of Things, " Transactions on Emerging Telecommunications Technologies, vol. 32, no. 6, Nov. 2020, doi: 10.1002/ett.4158.

[9] A. Erola, I. Agrafiotis, M. Goldsmith, and S. Creese, "Insider-threat detection: Lessons from deploying the CITD tool in three multinational organisations," Journal of Information Security and Applications, vol. 67, p. 103167, Jun. 2022, doi: 10.1016/j.jisa.2022.103167.

[10] R. Chinchani, A. Iyer, H. Q. Ngo, and S. Upadhyaya, "Towards a Theory of Insider Threat Assessment," 2005 International Conference on Dependable Systems and Networks (DSN'05), 2022, doi: 10.1109/dsn.2005.94.

[11] G. Deep, J. Sidhu, and R. Mohana, "Insider threat prevention in distributed database as a service cloud environment," Computers & Industrial Engineering, vol. 169, p. 108278, Jul. 2022, doi: 10.1016/j.cie.2022.108278.

[12] S. Shah et al., "Compromised user credentials detection in a digital enterprise using behavioral analytics," Future Generation Computer Systems, vol. 93, pp. 407–417, Apr. 2019, doi: 10.1016/j.future.2018.09.064.

[13] "Detection of Compromised Online Social Network Account with an Enhanced Knn," Applied Artificial Intelligence, vol. 34, no. 11, pp. 777-791, 2020, doi: 10.1080/08839514.2020.1782002.

[14] "Compromised Accounts Detection Based on Information Entropy," International Journal of Network Security, Vol.23, No.3, PP.401-411, May 2021 doi: 10.6633/IJNS.202105 23(3).05.

[15] I. Herrera Montano, J. J. García Aranda, J. Ramos Diaz, S. Molina Cardín, I. de la Torre Díez, and J. J. P. C. Rodrigues, "Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat," Cluster Computing, Jul. 2022, doi: 10.1007/s10586-022-03668-2.

[16] Software Engineering Institute, "Insider Threat Test Dataset," Carnegie Mellon University, Nov. 2016. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508099 (accessed Oct. 23, 2022).

[17] Kim, Park, Kim, Cho, and Kang, "Insider Threat Detection Based on User Behavior Modeling and Anomaly Detection Algorithms," Applied Sciences, vol. 9, no. 19, p. 4018, Sep. 2019, doi: 10.3390/app9194018.

[18] C.-L. Li, K. Sohn, J. Yoon, and T. Pfister, "CutPaste: Self-Supervised Learning for Anomaly Detection and Localization," Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pp. 9664–9674, 2021, Available: https://openaccess.thecvf.com/content/CVPR2021/html/Li_CutPaste_Self-Supervised_Learning_for_Anomaly_Detection_and_Localization_CVPR_2021_paper.html

[19] L. Ruff et al., "A Unifying Review of Deep and Shallow Anomaly Detection," Proceedings of the IEEE, vol. 109, no. 5, pp. 756–795, May 2021, doi: 10.1109/jproc.2021.3052449.

[20] S. Cai et al., "An efficient outlier detection method for data streams based on closed frequent patterns by considering anti-monotonic constraints," Information Sciences, vol. 555, pp. 125–146, May 2021, doi: 10.1016/j.ins.2020.12.050.

[21] M. N. Al-Mhiqani et al., "A new intelligent multilayer framework for insider threat detection," Computers & Electrical Engineering, vol. 97, p. 107597, Jan. 2022, doi: 10.1016/j.compeleceng.2021.107597.

[22] N. J. Camp and A. D. Williams, "Lessons Learned from a Comparative Analysis of Counterintelligence and Insider Threat Mitigation Case Studies in Nuclear Facilities," SN Computer Science, vol. 3, no. 2, Jan. 2022, doi: 10.1007/s42979-021-00996-9.

[23] Z. Zhang, H. Wang, J. Geng, W. Jiang, X. Deng, and W. Miao, "An information fusion method based on deep learning and fuzzy discount-weighting for target intention recognition," Engineering Applications of Artificial Intelligence, vol. 109, p. 104610, Mar. 2022, doi: 10.1016/j.engappai.2021.104610.

[24] M. Yildirim and E. Anarim, "Mitigating insider threat by profiling users based on mouse usage pattern: ensemble learning and frequency domain analysis," International Journal of Information Security, vol. 21, no. 2, pp. 239–251, May 2021, doi: 10.1007/s10207-021-00544-9.

[25] B. Manral and G. Somani, "Establishing forensics capabilities in the presence of superuser insider threats," Forensic Science International: Digital Investigation, vol. 38, p. 301263, Sep. 2021, doi: 10.1016/j.fsidi.2021.301263.

[26] M. Jeong and H. Zo, "Preventing insider threats to enhance organizational security: The role of opportunity-reducing techniques," Telematics and Informatics, vol. 63, p. 101670, Oct. 2021, doi: 10.1016/j.tele.2021.101670.

[27] K. Björkman, J.-E. . Holmberg, and T. Mätäsniemi, "Comparing physical protection strategies against insider threats using probabilistic risk assessment," Nuclear Engineering and Design, vol. 391, p. 111738, May 2022, doi: 10.1016/j.nucengdes.2022.111738.

[28] K. Kisenasamy, S. Perumal, V. Raman, and B. S. M. Singh, "Influencing factors identification in smart society for insider threat in law enforcement agency using a mixed method approach," International Journal of System Assurance Engineering and Management, vol. 13, no. S1, pp. 236–251, Nov. 2021, doi: 10.1007/s13198-021-01378-3.

[29] Le, Duc C., and A. Nur Zincir-Heywood. "Machine learning based insider threat modelling and detection," IFIP/IEEE Symposium on Integrated Network and Service Management (IM), pp. 1-6, 2019.

[30] C. Soh, S. Yu, A. Narayanan, S. Duraisamy, and L. Chen, "Employee profiling via aspect-based sentiment and network for insider threats detection," Expert Systems with Applications, vol. 135, pp. 351–361, Nov. 2019, doi: 10.1016/j.eswa.2019.05.043.

[31] M. Singh, B. Mehtre, and S. Sangeetha, "User behavior based Insider Threat Detection using a Multi Fuzzy Classifier," Multimedia Tools and Applications, vol. 81, no. 16, pp. 22953–22983, Mar. 2022, doi: 10.1007/s11042-022-12173-y.

[32] E. Alhajjar and T. Bradley, "Survival analysis for insider threat," Computational and Mathematical Organization Theory, Jul. 2021, doi: 10.1007/s10588-021-09341-0.

[33] Y. Wei, K.-P. Chow, and S.-M. Yiu, "Insider threat prediction based on unsupervised anomaly detection scheme for proactive forensic investigation," Forensic Science International: Digital Investigation, vol. 38, p. 301126, Oct. 2021, doi: 10.1016/j.fsidi.2021.301126.

[34] U. Rauf, M. Shehab, N. Qamar, and S. Sameen, "Formal approach to thwart against insider attacks: A bio-inspired auto-resilient policy regulation framework," Future Generation Computer Systems, vol. 117, pp. 412–425, Apr. 2021, doi: 10.1016/j.future.2020.11.009.

[35] J. Chen, S. Yuan, D. Lv, and Y. Xiang, “A novel self-learning feature selection approach based on feature attributions,” Expert Systems with Applications, vol. 183, p. 115219, Nov. 2021, doi: 10.1016/j.eswa.2021.115219.

[36] H. Guo, S. Yuan, and X. Wu, “LogBERT: Log Anomaly Detection via BERT,” 2021 International Joint Conference on Neural Networks (IJCNN), Jul. 2021, doi: 10.1109/ijcnn52387.2021.9534113.

[37] P. Zheng, S. Yuan, and X. Wu, “Using Dirichlet Marked Hawkes Processes for Insider Threat Detection,” Digital Threats: Research and Practice (DTRAP), vol. 3, pp. 1-19, March 2022. doi: 10.1145/3457908

[38] S. Yuan, P. Zheng, X. Wu, H. Tong, “Few-shot Insider Threat Detection,” Proceedings of the 29th ACM International Conference on Information & Knowledge Management, p. 2289-2292, Oct. 2020, doi: 10.1145/3340531.3412161

[39] S. Yuan, P. Zheng, X. Wu, and Q. Li, “Insider Threat Detection via Hierarchical Neural Temporal Point Processes,” 2019 IEEE International Conference on Big Data (Big Data), Dec. 2019, doi: 10.1109/bigdata47090.2019.9005589.

[40] P. Zheng, S. Yuan, and X. Wu, “SAFE: A Neural Survival Analysis Model for Fraud Early Detection,” Proceedings of the AAAI Conference on Artificial Intelligence, vol. 33, pp. 1278–1285, Jul. 2019, doi: 10.1609/aaai.v33i01.33011278.

[41] P. Zheng, S. Yuan, X. Wu, J. Li, and A. Lu, “One-Class Adversarial Nets for Fraud Detection,” Proceedings of the AAAI Conference on Artificial Intelligence, vol. 33, pp. 1286–1293, Jul. 2019, doi: 10.1609/aaai.v33i01.33011286.

[42] D. Xu, S. Yuan, L. Zhang, and X. Wu, “FairGAN: Fairness-aware Generative Adversarial Networks,” 2018 IEEE International Conference on Big Data (Big Data), Dec. 2018, doi: 10.1109/bigdata.2018.8622525.

[43] S. A. Soleymani et al., “An authentication and plausibility model for big data analytic under LOS and NLOS conditions in 5G-VANET,” Science China Information Sciences, vol. 63, no. 12, Nov. 2020, doi: 10.1007/s11432-019-2835-4.

[44] S. Chouaibi, G. Festa, R. Quaglia, and M. Rossi, “The risky impact of digital transformation on organizational performance – evidence from Tunisia,” Technological Forecasting and Social Change, vol. 178, p. 121571, May 2022, doi: 10.1016/j.techfore.2022.121571.

[45] D. Li, L. Yang, H. Zhang, X. Wang, and L. Ma, “Memory-Augmented Insider Threat Detection with Temporal-Spatial Fusion,” Security and Communication Networks, vol. 2022, pp. 1–19, Apr. 2022, doi: 10.1155/2022/6418420.

[46] R. G. Gayathri, A. Sajjanhar, and Y. Xiang, “Hybrid Deep Learning Model using SPCAGAN Augmentation for Insider Threat Analysis,” arXiv.org, 2022, doi: 10.48550/arXiv.2203.02855.

[47] S. Cai et al., “An efficient anomaly detection method for uncertain data based on minimal rare patterns with the consideration of anti-monotonic constraints,” Information Sciences, vol. 580, pp. 620–642, Nov. 2021, doi: 10.1016/j.ins.2021.08.097.

[48] S. Cai et al., “MWFP-outlier: Maximal weighted frequent-pattern-based approach for detecting outliers from uncertain weighted data streams,” Information Sciences, vol. 591, pp. 195–225, Apr. 2022, doi: 10.1016/j.ins.2022.01.028.

[49] K. Roth, L. Pemula, J. Zepeda, B. Schölkopf, T. Brox, and P. Gehler, “Towards Total Recall in Industrial Anomaly Detection,” Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pp. 14318–14328, 2022, Available: https://openaccess.thecvf.com/content/CVPR2022/html/Roth_Towards_Total_Recall_in_Industrial_Anomaly_Detection_CVPR_2022_paper.html

[50] D. C. Le and N. Zincir-Heywood, “Anomaly Detection for Insider Threats Using Unsupervised Ensembles,” IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1152–1164, Jun. 2021, doi: 10.1109/tnsm.2021.3071928.

[51] D. C. Le and N. Zincir - Heywood, “Exploring anomalous behaviour detection and classification for insider threat identification,” International Journal of Network Management, vol. 31, no. 4, Mar. 2020, doi: 10.1002/nem.2109.

[52] M. Chowdhury, B. Ray, S. Chowdhury, S. Rajasegarar, “A Novel Insider Attack and Machine Learning Based Detection for the Internet of Things,” ACM Transactions on Internet of Things, vol. 2, no. 26, pp. 1-23, Nov. 2021, doi: 10.1145/3466721

[53] A. Wall and I. Agrafiotis, “A Bayesian approach to insider threat detection,” Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 12, no. 2, 2021, doi: 10.22667/JOWUA.2021.06.30.048

[54] S. Wasko et al., “Using alternate reality games to find a needle in a haystack: An approach for testing insider threat detection methods,” Computers & Security, vol. 107, p. 102314, Aug. 2021, doi: 10.1016/j.cose.2021.102314.

[55] R. G. Gayathri, A. Sajjanhar, Y. Xiang, and X. Ma, “Anomaly Detection for Scenario-based Insider Activities using CGAN Augmented Data,” 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Oct. 2021, doi: 10.1109/trustcom53373.2021.00105.

[56] A. Subhani, I. A. Khan, and A. Zubair, “Review of insider and insider threat detection in the organizations,” Journal of Advanced Research in Social Sciences and Humanities, vol. 6, no. 4, pp. 167–174, 2021, Available: https://jarssh.com/ojs/index.php/jarssh/article/view/174

[57] A. D. Williams, S. N. Abbott, N. Shoman, and W. S. Charlton, “Results From Invoking Artificial Neural Networks to Measure Insider Threat Detection & Mitigation,” Digital Threats: Research and Practice, vol. 3, no. 3, pp. 1-20, Oct. 2021, doi: 10.1145/3457909

[58] A. S. Anakath, R. Kannadasan, N. P. Joseph, P. Boominathan, and G. R. Sreekanth, ”Insider Attack Detection Using Deep Belief Neural Network in Cloud Computing. ” Computer Systems Science & Engineering, pp. 479-492, 2022, doi: 10.32604/csse.2022.019940

[59] X. Wang, C. Fidge, G. Nourbakhsh, E. Foo, Z. Jadidi, and C. Li, “Anomaly Detection for Insider Attacks From Untrusted Intelligent Electronic Devices in Substation Automation Systems,” IEEE Access, vol. 10, pp. 6629–6649, 2022, doi: 10.1109/access.2022.3142022.

[60] G.-M. Go, S.-J. Bu, and S.-B. Cho, “Insider attack detection in database with deep metric neural network with Monte Carlo sampling,” Logic Journal of the IGPL, Feb. 2022, doi: 10.1093/jigpal/jzac007.

[61] I. F. Kilincer, F. Ertam, and A. Sengur, “Machine learning methods for cyber security intrusion detection: Datasets and comparative study,” Computer Networks, vol. 188, p. 107840, Apr. 2021, doi: 10.1016/j.comnet.2021.107840.

[62] R. Nasir, M. Afzal, R. Latif, and W. Iqbal, “Behavioral Based Insider Threat Detection Using Deep Learning,” IEEE Access, vol. 9, pp. 143266–143274, 2021, doi: 10.1109/access.2021.3118297

[63] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, “Systematic literature reviews in software engineering – A systematic literature review,” Information and Software Technology, vol. 51, no. 1, pp. 7–15, Jan. 2009, doi: 10.1016/j.infsof.2008.09.009.