Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 12, Issue. 4, April 2023, pg.60 – 88

Systematic Literature Review and Metadata Analysis of Insider Threat Detection Mechanism

Ismaila Idris; Adeleke Nafisa Damilola
Department of Cyber Security Science, Federal University of Technology, Minna, Niger State, Nigeria
DOI: https://doi.org/10.47760/ijcsmc.2023.v12i04.007

ABSTRACT:
Insider threat refers to the risk caused to an organization's security, assets, or data by individuals who have authorized access to these resources, such as employees, contractors, or partners. The aim of an insider threat is usually to exploit their access to sensitive information or systems to carry out malicious activities, such as stealing intellectual property, financial data, or sensitive information, sabotaging systems, or processes, or committing fraud. This systematic literature analysed the anatomy of insider threat, including its trends and mode of attacks to find the possible solutions by querying various academic literature. Sources of insider threat dataset are revealed in this review paper to ease the challenges of researchers in getting access to insider datasets. In addition, a taxonomy of insider threat current trends is presented in the paper. This review can serve as a benchmark for researchers in proposing a novel insider threat detection methodology and starting point for novice researchers.
Keywords: Insider Threat; Insider Threat Trends; Insider Threat detection

I. INTRODUCTION

Insider threat refers to the risk caused to an organization's security, assets, or data by individuals who have authorized access to these resources, such as employees, contractors, or partners. This risk can arise from insiders' intentional or unintentional actions, such as stealing sensitive information, sabotaging operations, or simply making mistakes that compromise the organization's security. Insider threats are particularly dangerous because insiders typically have intimate knowledge of the organization's vulnerabilities, assets, and

operations, making it easier for them to carry out attacks or avoid detection (Greitzer Deborah A., 2010).

Insider threats can take on various forms, such as violence, espionage, sabotage, theft, and cyber acts. In detail, violence may involve threatening behaviours that create a hostile or abusive environment, while espionage may refer to spying practices to gain confidential information for military, political, or financial advantage. Sabotage involves deliberate actions to harm an organization's infrastructure, including physical and virtual means, while theft may include unauthorized taking of money or intellectual property. Lastly, cyber acts involve stealing, espionage, violence, and sabotage in relation to technology, devices, or the internet. Unintentional threats may also arise from non-malicious exposure of IT infrastructure, while intentional threats are malicious actions that use technical means to disrupt regular business operations, gain protected information, or execute an attack plan (CISA, 2022).

The aim of an insider threat is usually to exploit their access to sensitive information or systems to carry out malicious activities, such as stealing intellectual property, financial data, or sensitive information, sabotaging systems, or processes, or committing fraud. In some cases, the insider threat may be motivated by personal gain, revenge, ideology, or simply negligence. The impact of an insider threat can be severe, leading to financial loss, reputational damage, and legal liability for the organization. Therefore, organizations need to implement effective security measures to detect, prevent, and mitigate the risk of insider threats.

The increase in insider threat incident prompted researchers to deploy efforts in order to find an effective solution to these attacks being perpetrated by the insider threat (Axelrad et al., 2013; J Liu et al., 2023; M Singh et al., 2023). In turn, the proposed solutions are expected to drastically reduce its negative impact, reduce the false alarm, and increase it detection rate. As a result of finding solution to insider threat, analysis on insider threat flooded the literature. However, lasting solution to insider threat is yet to become a reality despite that researchers have deployed the massive efforts (Axelrad et al., 2013; Michael and Eloff, 2019; Pal et al., 2023; Prasad et al., 2009; Sharma et al., 2020).

There are previous systematic reviews on insider threat in the literature. However, the major issue with those previous reviews is that they mainly concentrated on insider threat in healthcare sectors and some other specific areas. In this paper, we propose to conduct a

comprehensive systematic review of all analysis carried out on insider threat activities which include its attack model, types, detection and protection of users, facilities, infrastructure, and environment.

The purpose for this review work is to have a clear view on the mode of attack, structure, and the behaviour of various insider threat, to understand the factors that made insider threat to grow, and to see what the experts' researchers are saying and doing to curtail the excesses of insider threat. The major contributions of the paper are as follows:

1. We analyzed the parameters used for the evaluation of insider threat attack, and detection mechanisms.
2. We summarized and tabulate all available research datasets for future analysis of insider threat anatomy.
3. We present a systematic literature review of insider threat detection mechanisms.

The remaining parts of the paper are organized as follows: Sect. 2 presents a detailed analysis of previous related surveys. Section 3 details the research methodology, whereas Sect. 4 the analysis of datasets used for insider threat. Further discussion was done in Sect. 5 before concluding the paper in Sect. 6.

II. PREVIOUS RELATED SURVEYS

This section presents previous related surveys in the area of insider threat research as shown in Table 2. The authors (AP Singh and Sharma, 2022) provided a systematically review on insider threats and its detection, while highlighting the main types and method to minimized insider threat attack.

(Al-mhiqani et al., 2020) present a taxonomy of contemporary insider types, access, level, motivation, insider profiling, effect security property, and methods used by attackers to conduct attacks and analysed behaviours, machine-learning techniques, dataset, detection methodology, and evaluation metrics. Figure 1 shows the number of articles in each database sources considered for the systematic review.

A review of insider threat detection approaches was carry out by (Kim et al., 2020) carry out a research how insider threat data should be collected and utilized in the industry to detect insider threats in the Internet of Things (IoT) environment.

The survey carried out by (S Yuan and Wu, 2021) on the application of deep learning techniques to insider threat detection, review the current developments and potential future directions of insider threat detection using deep learning, and its application on anomaly detection, as well as identification and classification of challenges.

In the paper of (Kim et al., 2019), the authors provided a systematic understanding of the past literature that addresses the issues with insider threat detection by examining the different types of insider threats based on insider characteristics and insider activities, explored the sensors which make possible detecting insider threats in an automated way, and the public datasets available for research.

The work of (Walker-Roberts et al., 2018) conducted a systematic review on insider threat detection; however, the scope of the review focused only on insider threats in the healthcare critical infrastructures.

(Nazir Shushma; Patel, Dilip, 2017) provided a comprehensive study on modelling, simulation, and related techniques that have been used to assess the vulnerabilities of the supervisory control and data acquisition (SCADA) system to cyberattacks.

The research work done by (Rose *et al.,* 2017) proposed a distributed, automated detection system among endpoint host machines with a centralized repository.

A survey was carried out by (Jiang et al., 2016) regarding the machine-learning techniques that can be utilized for various computer security domains, including intrusion detection systems, software security, security policy management, identification of malware, mitigation of malware et cetera.

A study (Sanzgiri and Dasgupta, 2016) further divides the insider threat detection techniques into nine classes: (1) anomaly-based approaches; (2) role-based access control; (3) scenario-based techniques; (4) decoy documents and honeypot techniques; (5) risk analysis using psychological factors; (6) risk analysis using workflow; (7) improving network defence; (8) improving defence by access control; and (9) process control to deter insiders.

In the study done by (Gheyas Ali E. et al., 2016), they found that the most popular research trends in the field as follows: dataset- game theory approach (GTA), feature-insider's online activities, and algorithm-graph algorithm.

Table 1: Related Surveys on Insider Threat

S/N	Reference	No of references covered
1	(Velayudhan et al., 2023)	15
2	(AP Singh and Sharma, 2022)	14
3	(S Yuan and Wu, 2021)	17
4	(Al-mhiqani et al., 2020)	13
5	(Kim et al., 2020)	11
6	(Homoliak et al., 2019)	12
7	(Kim et al., 2019)	14
8	(Walker-Roberts et al., 2018)	16
9	(L Liu et al., 2018)	18
10	(Nazir Shushma; Patel, Dilip, 2017)	15
11	(Rose et al., 2017)	15
12	(H Jiang et al., 2016)	17
13	(Sanzgiri and Dasgupta, 2016)	19
14	(Gheyas Ali E. et al., 2016)	14
15	(Azaria Ariella; Kraus, Sarit; Subrahmanian, V. S. et al., 2014)	13

III. RESEARCH METHODOLOGY

The research methodology section presents the research steps followed to review the existing works in the area of insider threat attack and detection systems. We also explain the selection of the existing studies which was done through a set inclusion and exclusion criteria.

3.1 Protocol and Phases of the Study

The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) (Moher et al., 2009) and the established guidelines in the work of (Kitchenham et al., 2009) were adopted in the course of this review.

3.2 Search and Data Sources

Several databases were queried to gather appropriate literature related to insider threat, and defend techniques. The articles were properly scrutinized using identification of primary studies with other different techniques. The research procedure adopted in this article spanned through relevant papers from a variety of academic databases including ACM Digital Library, IEEE Xplore, Science Direct, Springer, Taylor & Francis, Web of Science and Wiley Online Library as shown in Table 2.

Table 2: Search Database Sources

S/N	Database Name	No of Article
1	IEEE Xplore	103
2	ScienceDirect	156
3	Springer	98
4	Taylor & Francis	54
5	Web of Science	12
6	Wiley Online Library	56
7	ACM Digital Library	60
Total		539

3.3 Search Keyword

The primary search terms were carefully selected to ascertain the most appropriate search terms. Using the review set goals, the following terms were applied to search the relevant literature in some reputable academic archives: 'Insider threat, 'Insider threat + defend', 'Cyber incident + insider threat, 'Cyber-attack + insider threat. Figure 2 shows the number of insider threat published articles per year.

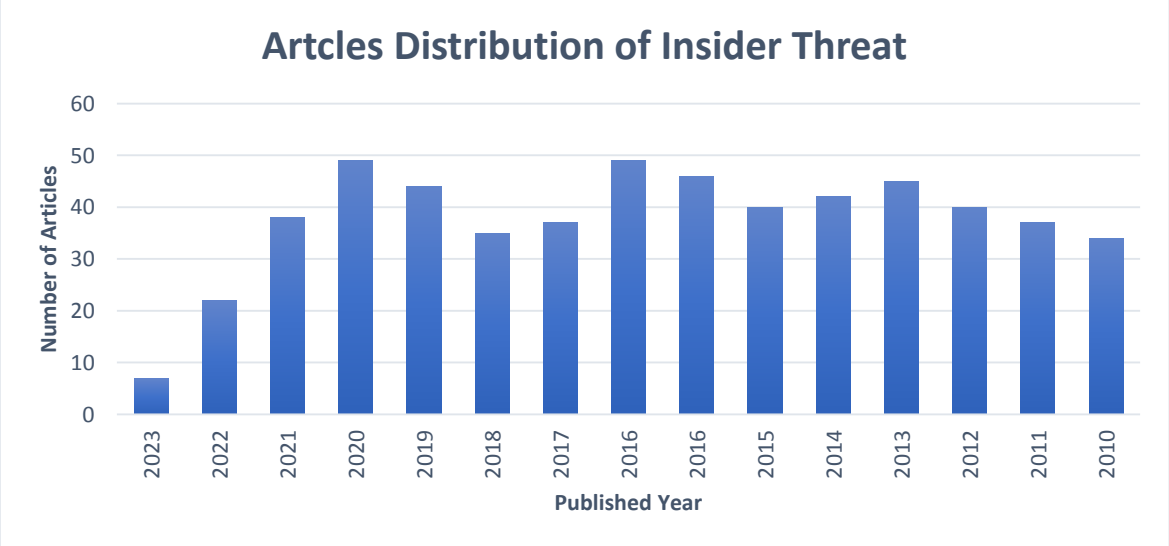

Figure 1: Number of Insider Threat Published Articles Per Years

3.4 Inclusion and Exclusion Criteria for the Study

The study utilized the five-point criteria in the determination of the eligibility of research publications to be selected in the review. The criteria and matching justification are shown in table 3.

Table 3: Criteria for the article inclusion and exclusion of research publications

S/N	Criteria	Explanation/justification
1	Original research publication, not a review or survey paper	The research papers are expected to discuss insider threat, and insider threat detection mechanism.
2	The proposed solutions must be capable of detecting or predicting insider threat	The aim of this research is to aid novice and expert researcher in the development of better safety techniques and approaches
3	The publication must be full-length paper	Short papers are insufficient in providing relevant information on the proposed solution
4	The language chosen for writing the articles must be English language	The publication must be made is English language
5	The paper must be published between 2010 -2023	The coverage of the Systematic Literature Review is 12 years, from 2010 – 2023

3.5 Data Collection and Synthesis of Results

The articles reviewed are in consonant with the reality of the day, acknowledging the growing threat of insider threat in today world. The devastating effect on information and infrastructures of companies and organizations has led to huge losses. Dealing with the threats has become a mirage of nightmare to the information security experts. The two strong drivers that led to the growth of insider threat include the ever-changing technological landscape where new information technology systems are fast implemented as compared to the security components which are meant to protect them, and lack of policy initiative, proper understanding, and training of the end users on the use and application of information technology facilities.

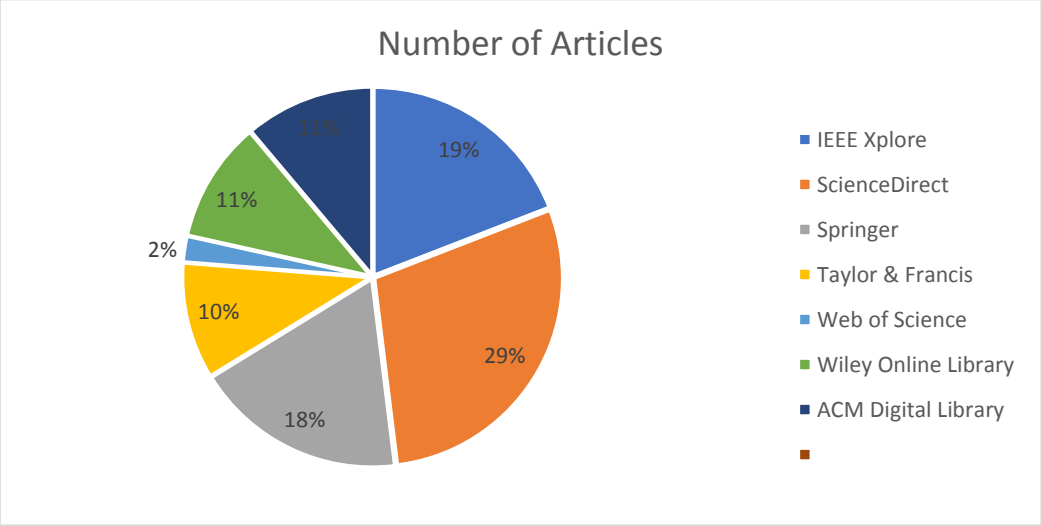

Figure 2: Number of Articles Per Journal Database

3.6 Study Selections Processes

There was a total of 565 studies identified by the initial keyword searches on the chosen platforms. After eliminating the duplicate research, this number was drastically reduced to 200. The research that met the inclusion/exclusion criteria were thoroughly examined, and 167 publications were left over for reading. Only papers written in English and published between 2010 – 2023 were chosen. After reading all 167 papers in detail and using the inclusion/exclusion criteria once again, 75 papers were left for the systematic literature review in the end. The identification, screening, eligibility and included phases are shown in Figure 3.

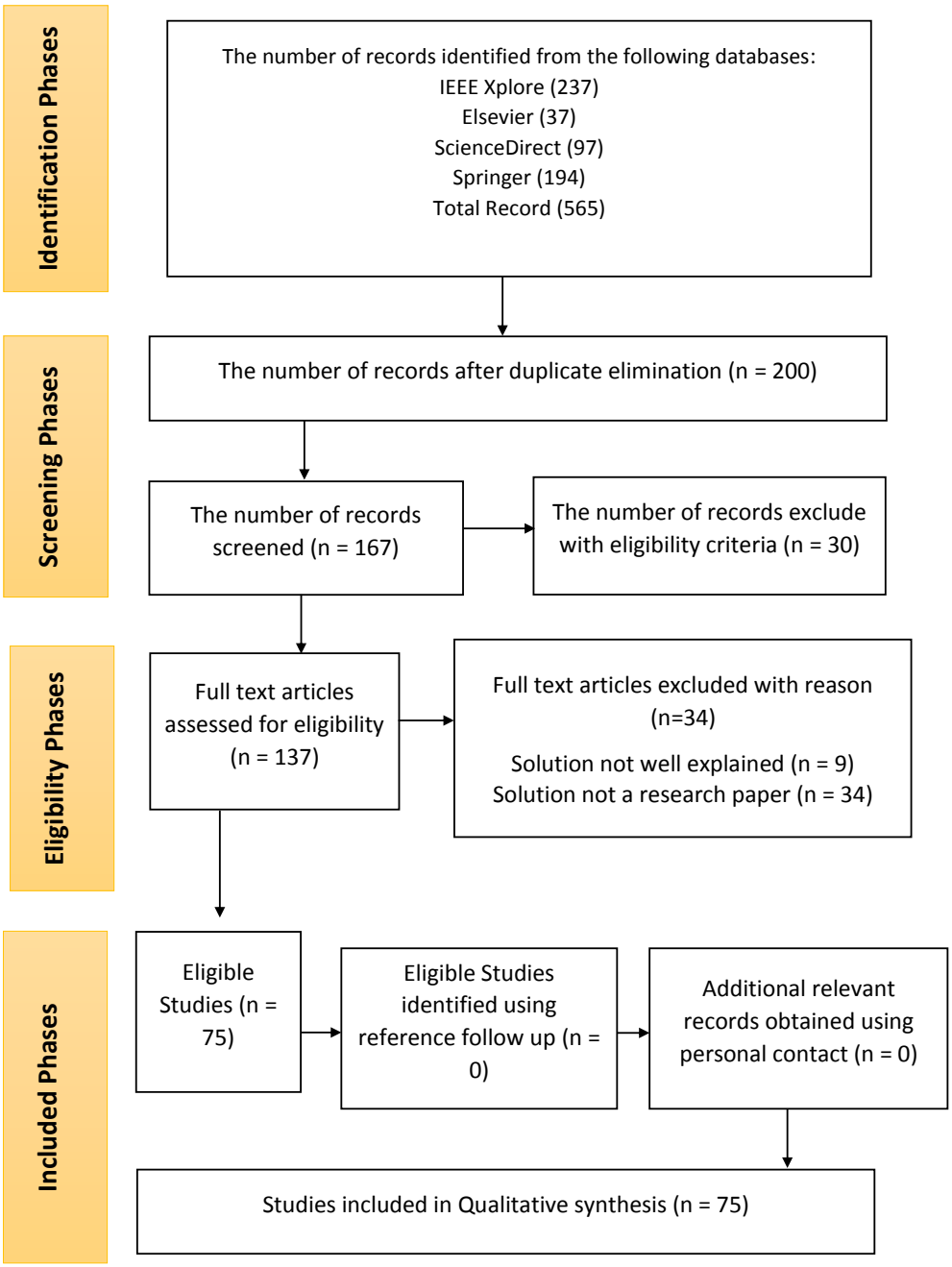

Figure 3: The Study Selection Workflow with Prisma

IV. SYNTHESES OF INSIDER THREAT DETECTION TECHNIQUES

Two deep learning hybrid LSTM models integrated with Google's Word2vec LSTM (Long Short-Term Memory) GLoVe (Global Vectors for Word Representation) LSTM for detecting insider threats was proposed in (Haq et al., 2022). The models were evaluated using a real dataset, and the results showed that the ML-based models outperformed the DL-based ones. The models were compared with state-of-the-art ML models such as XGBoost, Ada-Boost, RF (Random Forest), KNN (K-Nearest Neighbour), and LR (Logistics Regression). The paper highlights the importance of pre-trained word embeddings in NLP models for detecting the semantic and syntactic value of the word vector. The limitations addressed in the paper are the availability of a limited volume of real data, ethical and privacy issues, and the high volume of data requiring good computation.

Supervised insider threat detection method based on ensemble learning and self-supervised learning to detect malicious session which uses TF-IDF feature extraction and over-bootstrap sampling to improve the detection effect was proposed in (Zhang et al., 2021). The experimental results show that the proposed method can effectively detect malicious sessions in CERT4.2 and CERT6.2 datasets, with AUCs of 99.2% and 95.3% in the best case. The paper also shows that the proposed ensemble learning and self-supervised learning methods, as well as the TF-IDF feature extraction method, can improve the effectiveness of insider threat detection.

The paper (Li et al., 2021) Proposed an image-based classification method for insider threat detection. The techniques used in this method include feature extraction, image conversion, and a modified unsupervised anomaly detection algorithm. The feature extraction step involves extracting relevant information from the images, while the image conversion step converts the extracted features into a format that can be used for anomaly detection. The

modified unsupervised anomaly detection algorithm is used to detect any abnormal behaviour in the user's actions.

(D Sun and Wang, 2021) paper Proposed a framework called DeepMIT for detecting malicious insider threats. The framework uses Recurrent Neural Networks to model user behaviours as time sequences and predict the probabilities of anomalies. It also includes user-attributes information to provide precise context, which helps identify users' truly typical behaviour. The framework allows for real-time learning and detection of anomalies, and provides further insight into the anomaly scores to help operators quickly take further steps. The experimental evaluations over a public insider threat dataset have demonstrated that DeepMIT outperforms other existing malicious insider threat solutions.

The author (Wall and Agrafiotis, 2021) discusses the problem of insider attacks on organizations, where rogue employees with legitimate access to systems can evade detection and cause harm and how traditional security controls and detection systems are not effective in detecting such attacks. The paper proposes a Bayesian Network architecture that considers both network data and behavioural aspects to detect insider threats so as to understand the structure of the data and inputs specially crafted features based on theoretical foundations of insider threat. The proposed approach was evaluated on a synthetic dataset and showed high effectiveness in identifying all attacks with a very low number of false positives.

The research paper (Nasser Al-Mhiqani et al., 2021) proposed a new model called AD-DNN, which uses a combination of adaptive synthetic sampling and deep neural network techniques to improve the detection of insider threats. The proposed model is evaluated using the CERT dataset, and the results show that it outperforms existing insider threat detection systems. The paper highlights the importance of addressing the issue of imbalanced data in insider threat detection and suggests that the proposed model can be a promising solution to this problem.

A new method for detecting and diagnosing faults in wind turbines using machine learning algorithms in (Nasir et al., 2021) which involves collecting data from various sensors installed on the wind turbine and using it to train a machine learning model. The model can then be used to detect and diagnose faults in real-time, allowing for timely maintenance and repair. The proposed method was tested on real-world wind turbines and was found to be effective in detecting and diagnosing faults.

This authors (Wei et al., 2021) proposed a novel unsupervised anomaly detection scheme based on cascaded autoencoders and joint optimization network for detecting insider threats in organizations. The proposed scheme is used for data purification among unlabelled digital evidence and joint optimization of the dimension reduction and density estimation network. The paper also uses a Bidirectional Long Short-Term Memory (BiLSTM) feature extractor for feature representation and a hypergraph correction module to solve the high false positive rate problem in insider threat detection. These techniques are used to design an end-to-end insider threat prediction framework for proactive forensic investigation. The proposed models are evaluated on public benchmark datasets and show superior performance among state-of-the-art baseline models.

This research paper (Nasser Al-Mhiqani et al., 2021) discusses the problem of insider threats in organizations, which can come from trusted employees. The paper proposes a new model called AD-DNN, which uses a combination of adaptive synthetic sampling and deep neural network techniques to improve the detection of insider threats. The proposed model is evaluated using the CERT dataset, and the results show that it outperforms current insider threat detection systems. The paper highlights the importance of addressing the issue of imbalanced data in insider threat detection and suggests that the proposed model can be a promising solution to this problem.

(Ma and Rastogi, 2020) propose a novel approach to detect insider threat using system logs and a special recurrent neural network (RNN) model. The proposed model achieves 93% prediction accuracy. The system logs are modelled as a natural language sequence, and patterns are extracted from these sequences. Workflows of sequences of actions that follow a natural language logic and control flow are created and assigned various categories of behaviours - malignant or benign. Any deviation from these sequences indicates the presence of a threat.

(Sheykhkanloo and Hall, 2020) focuses on detecting insider threats using machine learning algorithms. Insider threats can come in different forms such as malicious insiders, careless employees, and third-party contractors. The paper addresses the issue of an extremely imbalanced dataset and employs a balancing technique known as spread subsample. The results show that although balancing the dataset did not improve performance metrics, it did improve the time taken to build and test the model.

The authors (F Yuan et al., 2020) proposed a deep adversarial insider threat detection (DAITD) framework to handle the class imbalance problem in insider threat detection. The framework uses Generative Adversarial Networks (GAN) to generate high-quality synthetic samples that are close to the anomalous user behaviour. The proposed method outperforms other comparative inside threat detection algorithms.

In the paper (J Jiang et al., 2019) a graph convolutional network (GCN) based anomaly detection model was implemented to detect anomalous behaviours of users and malicious threat groups. The model considers both entities' properties and structural information between them to detect anomalous behaviours of individuals and associated anomalous groups. The proposed model is evaluated using a real-world insider threat data set and outperforms several state-of-art baseline methods. The paper also provides a general

framework of an anomaly detection system based on the GCN algorithm, which could be easily implemented and extended to other anomaly detection issues with high detection accuracy.

This paper (Le and Nur Zincir-Heywood, 2019) proposed a new framework for detecting insider threats using machine learning algorithms. The system uses data from activity logs and organization structure/user information to identify unknown malicious insiders. The study evaluates the system's performance on individual data instances as well as normal and malicious insiders. The results show that the machine learning-based detection system can learn from limited ground truth and detect new malicious insiders with high accuracy. Overall, the paper presents a user-centred approach to insider threat detection that can be useful for companies and government agencies.

(S Yuan et al., 2019) proposed a hierarchical neural temporal point process model for insider threat detection. The model combines temporal point processes and recurrent neural networks to capture the nonlinear dependency over the history of all activities. The model is capable of modelling activity times, activity types, session durations, and session intervals information. The lower-level of the model uses a seq2seq model with marked temporal point processes to capture intra-session information, while the upper-level LSTM predicts the interval of two sessions and the session duration based on activity history. Experimental results on two datasets demonstrate that the proposed model outperforms the models that only consider information of the activity types or time alone.

An anomaly detection framework to address the issue of high false alarms in detecting insider threats was proposed in (Haidar and Gaber, 2018). The framework consists of two components: one-class modelling and progressive update. The one-class modelling component applies class decomposition on normal class data to create k clusters, then trains

an ensemble of k base anomaly detection algorithms. The progressive update component updates each of the k models with sequentially acquired FP chunks, using an oversampling method to generate artificial samples for FPs per chunk, then retrains each model and adapts the decision boundary to reduce the number of future FPs. The proposed framework is tested on synthetic data sets and shows better performance in terms of F1 measure and fewer FPs compared to the base algorithms, as well as detecting all insider threats in the data sets.

A system for detecting insider threats in an organization using an ensemble of negative selection algorithms was proposed in (Igbe and Saadawi, 2018). The proposed system classifies user activities as either "normal" or "malicious." The effectiveness of the system is evaluated using case studies from the CERT synthetic insider threat dataset, and the results show that the proposed method is very effective in detecting insider threats. In summary, the paper proposes a method for detecting insider threats in an organization using an ensemble of negative selection algorithms, which is shown to be effective in detecting such threats.

(Haidar and Gaber, 2018) Proposed an anomaly detection framework to address the issue of high false alarms in detecting insider threats. The framework consists of two components: one-class modelling and progressive update. The one-class modelling component applies class decomposition on normal class data to create k clusters, then trains an ensemble of k base anomaly detection algorithms. The progressive update component updates each of the k models with sequentially acquired FP chunks, using an oversampling method to generate artificial samples for FPs per chunk, then retrains each model and adapts the decision boundary to reduce the number of future FPs. The proposed framework is tested on synthetic data sets and shows better performance in terms of F1 measure and fewer FPs compared to the base algorithms, as well as detecting all insider threats in the data sets.

(Goldberg et al., 2017) is about insider threat detection research, where a prototype system called PRODIGAL was developed and tested to explore different detection and analysis methods. The paper presents the data and test environment, system components, and the core method of unsupervised detection of insider threat leads. The paper also discusses a set of experiments evaluating the prototype's ability to detect both known and unknown malicious insider behaviours. The experimental results show the ability to detect a large variety of insider threat scenario instances imbedded in real data with no prior knowledge of what scenarios are present or when they occur. The paper describes the architecture of the prototype system and the environment in which the experiments were conducted.

A method called XABA for detecting insider threats in real-time without the need for contextual data entries or preprocessed user activity logs was proposed in (Zargar et al., 2016). XABA learns user roles and exclusive behaviours by analysing raw logs related to each network session of the user. It then checks for abnormal patterns and triggers the appropriate alert if any are found. The method is implemented on the big-stream platform to operate on high rates of network sessions. The paper presents a real traitor scenario to evaluate XABA, which is detected with low false positives. Overall, XABA can detect diverse types of scenarios in many contexts without any predefined information or preprocessed activity logs.

(Rashid et al., 2016) proposed a novel approach to detecting insider threats in organizations by using Hidden Markov Models (HMM) to learn a user's normal behaviour and detect anomalies in that behaviour. The paper provides evidence that this approach is successful at detecting insider threats and accurately learning a user's behaviour. The results show that the HMM is able to learn a user's behaviour and determine when the user deviates from that behaviour. The use of a HMM allows us to visualize the model and understand what the model deems as normal behaviour, which helps in identifying anomalous behaviour.

This research paper (Bin Ahmad et al., 2014) proposed a modified framework for detecting insider threats in organizations. The framework includes a fuzzy classifier and genetic algorithm to improve the accuracy of user behaviour categorization and reduce false alarms. The effectiveness of the modified framework has been verified through a scenario-driven approach and mathematical evaluation. The results show that the modified framework can accurately classify and detect users, which can help minimize false alarms. The paper suggests that this framework can be adopted by organizations with critical business operations.

Table 3: Syntheses of Insider Threat Detection Techniques

S/N	Reference	Techniques	Problem Addressed	Results/Findings	Limitation
1	(Haq *et al.,* 2022)	Long Short-Term Memory models integrated with Google's Word2vec and GLoVe (Global Vectors for Word Representation).	The paper addresses the limitations in detecting insider threats, by developing models for detecting insider threats using a real dataset, high accuracy, and significantly lower false alarm rate.	Word2ve was the lowest accuracy rate at 73.4% and GLoVe was slightly better at 74.58% with a loss value of 1.167 for GLoVe and 1.156 for Word2ve.	The volume of data was quite high; which makes computation complex. The literature focus on an insider threat dataset that is more of an email corporate fraud.
2	(Zhang et al., 2021)	TF-IDF + Over Booting + Self Supervised.	The paper addresses the problem of detecting insider threats in computer networks by improving the effectiveness of insider threat detection and mitigate the damage caused by insider attacks	A 65.5% false positive rate on 0.1 was recorded and 95.3% AUC.	The paper does not provide a detailed analysis of the proposed method, which may be a concern for large-scale deployments
3	(D Sun and Wang, 2021)	The paper Proposed a framework called DeepMIT which utilize Recurrent Neural Network (RNN), and user-attributes as categorical features	The paper addresses the issues of insider threats	93.2% was recorded for Recall, 91.6% for precision and 92.4% for f measure	The paper does not address the issue of false negatives
4	(Li et al., 2021)	The techniques used in this method include feature extraction, image	It addresses the problem of an approach that converts the	The results show that the proposed method outperforms existing	The proposed method may not be suitable for

		conversion, and a modified unsupervised anomaly detection algorithm.	unsupervised anomaly detection problem into a supervised image classification problem, thereby reducing the complexity of the detection process.	methods in terms of detection accuracy and false alarm rate	detecting advanced insider threats that involve sophisticated attack techniques.
5	(Nasir *et al.,* 2021)	This paper used LSTM-Autoencoder as the algorithm and	The paper addresses the problem of insider threat detection in networked systems of companies and government agencies.	The results show that the model can achieved 90.60% accuracy rate	The performance is dependent on the quality and quantity of the data used for training and testing
6	(Wei et al., 2021)	The paper Proposed a novel unsupervised anomaly detection scheme based on cascaded autoencoders (CAEs) and joint optimization network.	The paper addresses the problem of detecting insider threats via a proactive forensic investigation framework.	0.938 was recorded for Recall, 0.926 for precision and 0.932 for f1 score.	No accuracy rate is recorded.
7	(Le et al., 2020)	The paper Proposed a machine learning-based system for user centred insider threat detection which then analyses data on multiple levels of granularity to identify not only malicious behaviours but also malicious insiders.	The paper addresses the problem of insider threat detection in networked systems of companies and government agencies.	The results show that the machine learning-based detection system can detect up to 85% of malicious insiders at only a 0.78% false positive rate. The system is also able to quickly detect malicious behaviours, as low as 14 minutes after the first malicious action.	The proposed system does not address the issue of false negatives
8	(Ma and Rastogi, 2020)	The paper Proposed a novel	The paper addresses the	The proposed model	Relies on system

		approach that uses system logs to detect insider behaviour using a special recurrent neural network (RNN) model involving modelling system logs as a natural language sequence and extracting patterns from these sequences.	problem of insider threat detection in information communication technology to successfully detect only known types of anomalies from the log entries	achieved a 93% prediction accuracy rate.	logs to detect insider behaviour, and the proposed approach may require significant computational resources to process large amounts of system logs.
9	(Schuartz et al., 2020)	The authors have presented a large data stream detection and analysis distributed platform for detecting threats on the internet. The platform uses machine learning techniques for dimensionality reduction.	The problem addressed in this research is the detection of threats on the internet and the prevention of such attacks from occurring through the analysis of patterns and behaviour of the data stream in the network.		The paper does not provide information on the scalability of the proposed platform
10	(Sharma *et al.*, 2020)	The technique involves the use of LSTM-based Autoencoder to model user behaviour based on session activities while following a two-step process of calculating the reconstruction error using the autoencoder on the non-anomalous dataset and then using it to define the threshold to separate the	The paper addresses the problem of identifying anomalies from log data for insider threat detection,	The experimental results show that the model produced an Accuracy of 90.17%, True Positives of 91.03%, and False Positives of 9.84%.	High building features might lead to missing some key information and does not discuss the scalability of the proposed technique for large datasets.

		outliers from the normal data points.			
11	(Elmrabit, Yang, et al., 2020)	Random Forest		A 92.0% accuracy rate was achieved for both recall, precision, and f-score.	The accuracy rate fluctuates depending on the environment.
12	(Ferreira et al., 2019)	Feature normalization (scaling), Representation of explicit temporal information and Random Forest, Decision Tree, or Logistic Regression to evaluate the performance of the proposed techniques	Explores different techniques to leverage spatial and temporal characteristics of user behaviours to improve the performance of machine learning-based insider threat detection.	The results show that different feature normalization techniques and temporal information representation have varying effects on different classifiers. The Standard Scaler with Random Forest classifier produced the best performance.	The method is not robust for other machine learning classifier
13	(J Jiang et al., 2019)	Graph Convolutional Networks.		94.5% and 83.3% were recorded for accuracy and recall.	Take effect when detecting malicious groups in correlated anomalous events and groups.
14	(Tuor et al., 2017)	Deep and recurrent neural networks model are used to analyze system logs and identify potential cases of insider threat.	Focuses on the analysis of an organization's computer network activity as a key component of early detection and mitigation of insider threat.	The events labelled as insider threat activity in the dataset had an average anomaly score in the 95.53 percentile	The lack of a detailed analysis of computational resources required, and the issue of false positives not being addressed.

15	(Lin *et al.*, 2017)	The paper Proposed a hybrid model based on the deep belief network (DBN) and One-Class SVM (OCSVM) to detect insider threat. The DBN is used to extract hidden features from the multi-domain feature extracted by the audit logs, and the OCSVM is trained from the features learned by the DBN.	The paper addresses the problem of the existing work that mainly focused on the single pattern analysis of user single-domain behaviour, so as to improve the accuracy rate.	87.79% was recorded for the accuracy rate and 12.18% for the false positive rate.	Cannot handle temporal data and generates a large number of false alarms.
16	(L Sun et al., 2016)	These techniques introducing an extended version of the Isolation Forest algorithm for detecting anomalous user behaviour.	The goal of this paper is to raise an alarm to the system administrator and determine whether the behaviour constitutes an unauthorized or malicious use of a resource.	The literature obtained a recall of 98.92%, accuracy of 50.77%, 97.50%, true positive of 98.92%, false positive and 50.50% precision.	Each access log was considered an individual event.
17	(Azaria Ariella; Kraus, Sarit; Subrahmanian, V. S. et al., 2014)	Seven algorithms were developed and evaluated using the Behavioural Analysis of Insider Threat (BAIT) framework	The problem addressed in the paper is the issue of insider threat, which is receiving increasing attention within the computer science community as well as government and industry.	A recall of 0.6 with a precision of 0.3 was recorded.	The literature did not use an established dataset and does not address the issue of false positives.

V. SYNTHESES OF INSIDER THREAT DATASET

One of the major challenges faced in the analysis of insider threat are accessibility to essential datasets. Most of the research papers could not make available the sources of their dataset while some complained about lack of recent dataset to test their proposed model. However, recent dataset is very critical in evaluating newly proposed detection system because of the advancement of technology which renders old datasets irrelevant.

Table 4: Syntheses of Insider Threat Dataset

S/N	Reference	Enron corpus	CERT	NSLKDD OR KDD-99	Schonlau	RUU	The Wolf of SUTD	Vegas
1	(Haq et al., 2022)	√	√					
2	(Zhang et al., 2021)		√					
3	(D Sun and Wang, 2021)		√					
4	(Wei et al., 2021)			√				
5	(Nasir et al., 2021)		√					
6	(Sharma et al., 2020)		√					
7	(Soh et al., 2019)	√						
8	(Michael and Eloff, 2019)	√						
9	(J Jiang et al., 2019)		√					
10	(Meng et al., 2018)			√				
11	(F Yuan et al., 2018)		√					
12	(Lin et al., 2017)			√				
13	(Meryem Douzi; Bouabid, El Ouahidi; Mouad, Lemoudden, 2017)			√				
14	(Gamachchi and Boztaş, 2017)	√						
15	(Bose Bhargav R.; Tirthapura, Srikanta; Chung, Yung-Yu; Steiner, Donald, 2017)		√					
16	(Legg Oliver; Goldsmith, Michael; Creese, Sadie et al., 2017)		√					
17	(Neu et al., 2017)			√				
18	(Rashid et al., 2016)	√						
19	(Legg et al., 2016)		√					
20	(Gavai et al., 2015)			√				√
21	(Punithavathani et al., 2015)		√					
22	(Alguliev and Abdullaeva, 2014)					√		
23	(Young et al., 2013)		√					
24	(Salem Salvatore J., 2011)				√			
25	(Okolica et al., 2007)	√						

VI. SYNTHESES OF PARAMETER

In evaluating the performance analysis of the experiment, most researchers adopt various parameters in arriving at their decisions. Some of the metrics used include: Region of Convergence (ROC), Area under Curve (AUC), false-positive rate (FPR), accuracy, precision and recall as tabulated in the Table 5.

Table 5: Syntheses of Insider Threat Evaluation Metric

S/N	Reference	Accuracy	F Score	False Positive	Precision	Recall	AUC	ROC
1	(S et al., 2023)	√	√			√		
2	(Haq et al., 2022)		√		√	√		
3	(D Sun and Wang, 2021)		√		√	√		
4	(Wei et al., 2021)		√		√	√	√	
5	(Zhang et al., 2021)	√						
6	(Ma and Rastogi, 2020)	√						
7	(Nasser Al-Mhiqani et al., 2021)	√	√		√	√		
8	(Le and Zincir-Heywood, 2021)	√		√	√			
9	(Wall and Agrafiotis, 2021)		√		√	√		
10	(Li et al., 2021)	√		√				
11	(Elmrabit, Zhou, et al., 2020)	√	√		√	√		
12	(Le and Zincir-Heywood, 2020)						√	
13	(Lu and Wong, 2019)	√						
14	(Wang et al., 2018)	√	√					
15	(F Yuan et al., 2018)						√	
16	(Ha and Ryu, 2017)	√			√			
17	(Gavai et al., 2015)	√						√
18	(Alahmadi et al., 2015)	√	√		√	√		
19	(Azaria Ariella; Kraus, Sarit; Subrahmanian, V. S. et al., 2014)		√		√	√		

VII. CHALLENGES AND FUTURE RESEARCH DIRECTION

The average global cost of insider threat incidents has increased over the last two years from 8.76 million dollars in 2018 to 15.4 million dollars in 2022 with negligent insiders being the most common and accounting for 56% of all incidents costing an average of $484,931 per incident (Ponemon Institute, 2022) despite the number of researchers and solutions that had been developed over the years. This does not happen due to the absence of solutions, but challenges which prevent these solutions from being efficient, like advancement in technology, number of devices connected, inexperience of employers and employees.

An effective detection technique for insider threat should have the abilities to detect threat in real time while making sure the false alarm in not hindering the detection accuracy rate. Detecting insider threat with machine learning will no doubt go a long way but each technique here is highly dependent on the size and quality of the dataset and the experimental set up.

With any detection techniques, it should be able to give similar results even with changes in environment and this is possible when all logs are taking into consideration and the threat level is constantly updated. This detection system should utilize a method of dynamic and robust behaviour forecasting analysis together with intelligent machine learning to deliver predictive capabilities of insider threat detection.

One of the most effective strategies against insider threat is to stop employees from bringing their personal devices or accessing information in the organization with the private devices. This should be in conjunction with real time monitoring

VIII. CONCLUSIONS

In this paper, we present a systematic review on insider threat detection mechanism from 2010 to 2023 so as to provide an understanding for novice researcher interested in insider threat.

For this purpose, insider threat detection techniques have been examined, analysed, and surveyed. In future, it is expected to research and predict which detection technique would be useful and effective to combat insider threat.

REFERENCES

[1]. Al-mhiqani, M. N., Ahmad, R., Abidin, Z. Z., Yassin, W., Hassan, A., Abdulkareem, K. H., Ali, N. S., & Yunos, Z. (2020). A Review of Insider Threat Detection : Classification , Machine Learning Techniques , Datasets , Open Challenges , and Recommendations. *Applied Sciences*, *10*(15). https://doi.org/10.3390/app10155208

[2]. Alahmadi, B. A., Legg, P. A., & Nurse, J. R. C. (2015). Using internet activity profiling for insider-threat detection. *ICEIS 2015 - 17th International Conference on Enterprise Information Systems, Proceedings*, *2*, 709–720. https://doi.org/10.5220/0005480407090720

[3]. Alguliev, R., & Abdullaeva, F. (2014). Illegal Access Detection in the Cloud Computing Environment. *Journal of Information Security*, *05*(02), 65–71. https://doi.org/10.4236/jis.2014.52007

[4]. Axelrad, E. T., Sticha, P. J., Brdiczka, O., & Shen, J. (2013). A Bayesian network model for predicting insider threats. *Proceedings - IEEE CS Security and Privacy Workshops, SPW 2013*, 82–89. https://doi.org/10.1109/SPW.2013.35

[5]. Azaria Ariella; Kraus, Sarit; Subrahmanian, V. S., A. R., Azaria, A., Richardson, A., Kraus, S., & Subrahmanian, V. S. (2014). Behavioral Analysis of Insider Threat: A Survey and Bootstrapped Prediction in Imbalanced Data. *IEEE Transactions on Computational Social Systems*, *1*(2), 135–155. https://doi.org/10.1109/TCSS.2014.2377811

[6]. Bin Ahmad, M., Akram, A., Asif, M., & Ur-Rehman, S. (2014). Using genetic algorithm to minimize false alarms in insider threats detection of information misuse in windows environment. *Mathematical Problems in Engineering*, *2014*(i). https://doi.org/10.1155/2014/179109

[7]. Bose Bhargav R.; Tirthapura, Srikanta; Chung, Yung-Yu; Steiner, Donald, B. D. . A. (2017). Detecting Insider Threats Using RADISH: A System for Real-Time Anomaly Detection in Heterogeneous Data Streams. *IEEE Systems Journal*, *11*(2), 471–482. https://doi.org/10.1109/jsyst.2016.2558507

[8]. CISA. (2022). *Defining Insider Threats | CISA*. Webpage. https://www.cisa.gov/defining-insider-threats

[9]. Elmrabit, N., Yang, S. H., Yang, L., & Zhou, H. (2020). Insider Threat Risk Prediction based on Bayesian Network. *Computers and Security*, *96*. https://doi.org/10.1016/j.cose.2020.101908

[10]. Elmrabit, N., Zhou, F., Li, F., & Zhou, H. (2020, June 1). Evaluation of Machine Learning Algorithms for Anomaly Detection. *International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2020*. https://doi.org/10.1109/CyberSecurity49315.2020.9138871

[11]. Ferreira, P., Le, D. C., & Zincir-Heywood, N. (2019). Exploring Feature Normalization and Temporal Information for Machine Learning Based Insider Threat Detection. *15th International Conference on Network and Service Management, CNSM 2019*. https://doi.org/10.23919/CNSM46954.2019.9012708

[12]. Gamachchi, A., & Boztaş, S. (2017). Insider Threat Detection Through Attributed Graph Clustering. *2017 IEEE Trustcom/BigDataSE/ICESS*, 112–119.

[13]. Gavai, G., Sricharan, K., Gunning, D., Hanley, J., Singhal, M., & Rolleston, R. (2015). Detecting insider threat from enterprise social and online activity data. *MIST 2015 - Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats, Co-Located with CCS 2015*, 13–20. https://doi.org/10.1145/2808783.2808784

[14]. Gheyas Ali E., I. A. . A., Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider

threats to cyber security: a systematic literature review and meta-analysis. *Big Data Analytics*, *1*(1), 1–29. https://doi.org/10.1186/s41044-016-0006-0

[15]. Goldberg, H. G., Young, W. T., Reardon, M. G., Phillips, B. J., & Senator, T. E. (2017). Insider Threat Detection in PRODIGAL. *Hawaii International Conference on System Sciences*. https://www.forcepoint.com.

[16]. Greitzer Deborah A., F. L. . F. (2010). Insider Threats in Cyber Security - Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation. In *Insider Threats in Cyber Security* (Vol. 49, Issue NA). https://doi.org/10.1007/978-1-4419-7133-3_5

[17]. Ha, D., & Ryu, K. K. Y. (2017). 기계학습 기반 내부자위협 탐지기술: RNN Autoencoder를 이용한 비정상행위 탐지 Detecting Insider Threat Based on Machine Learning: Anomaly Detection Using RNN Autoencoder. *Journal of the Korea Institute of Information Security and Cryptology*, *27*(4), 763–773.

[18]. Haidar, D., & Gaber, M. M. (2018). Adaptive One-Class Ensemble-based Anomaly Detection: An Application to Insider Threats. *Proceedings of the International Joint Conference on Neural Networks*, *2018-July*. https://doi.org/10.1109/IJCNN.2018.8489107

[19]. Haq, M. A., Khan, M. A. R., & Alshehri, M. (2022). Insider Threat Detection Based on NLP Word Embedding and Machine Learning. *Intelligent Automation and Soft Computing*, *33*(1), 619–635. https://doi.org/10.32604/iasc.2022.021430

[20]. Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., Ochoa, M., Homoliak Flavio; Guarnizo, Juan; Elovici, Yuval; Ochoa, Martín, I. T., Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys*, *52*(2), 30–40. https://doi.org/10.1145/3303771

[21]. Igbe, O., & Saadawi, T. (2018). Insider Threat Detection using an Artificial Immune system Algorithm. *2018 9th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2018*, *November*, 297–302. https://doi.org/10.1109/UEMCON.2018.8796583

[22]. Jiang, H., Nagra, J., & Ahammad, P. (2016). *SoK: Applying Machine Learning in Security - A Survey*. http://arxiv.org/abs/1611.03186

[23]. Jiang, J., Chen, J., Gu, T., Choo, K.-K. R., Liu, C., Yu, M., Huang, W., Mohapatra, P., Raymond Choo, K.-K., Liu, C., Yu, M., Huang, W., & Mohapatra, P. (2019). Anomaly Detection with Graph Convolutional Networks for Insider Threat and Fraud Detection. In *IEEE Military Communications Conference*. https://doi.org/10.1109/MILCOM47813.2019.9020760.

[24]. Kim, A., Oh, J., Ryu, J., Lee, J., Kwon, K., & Lee, K. (2019). SoK: A systematic review of insider threat detection. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *10*(4), 46–67. https://doi.org/10.22667/JOWUA.2019.12.31.046

[25]. Kim, A., Oh, J., Ryu, J., & Lee, K. (2020). A review of insider threat detection approaches with IoT perspective. *IEEE Access*, *8*, 78847–78867. https://doi.org/10.1109/ACCESS.2020.2990195

[26]. Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering – A systematic literature review. *Information and Software Technology*, *51*(1), 7–15. https://doi.org/https://doi.org/10.1016/j.infsof.2008.09.009

[27]. Le, D. C., & Nur Zincir-Heywood, A. (2019). Machine learning based insider threat modelling and detection. *2019 IFIP/IEEE Symposium on Integrated Network and Service Management, IM 2019*, 1–6.

[28]. Le, D. C., & Zincir-Heywood, N. (2020). Exploring Adversarial Properties of Insider Threat Detection. *2020 IEEE Conference on Communications and Network Security, CNS 2020*. https://doi.org/10.1109/CNS48642.2020.9162254

[29]. Le, D. C., & Zincir-Heywood, N. (2021). Exploring anomalous behaviour detection and classification for insider threat identification. *International Journal of Network Management*, *31*(4), 1–19. https://doi.org/10.1002/nem.2109

[30]. Le, D. C., Zincir-Heywood, N., & Heywood, M. I. (2020). Analyzing Data Granularity Levels for Insider Threat Detection Using Machine Learning. *IEEE Transactions on Network and Service Management*, *17*(1), 30–44. https://doi.org/10.1109/TNSM.2020.2967721

[31]. Legg Oliver; Goldsmith, Michael; Creese, Sadie, P. A. . B., Legg, P. A., Buckley, O., Goldsmith, M., Creese, S., Legg Oliver; Goldsmith, Michael; Creese, Sadie, P. A. . B., Legg, P. A., Buckley, O., Goldsmith, M., & Creese, S. (2017). Automated Insider Threat Detection System Using User and Role-Based Profile Assessment. *IEEE Systems Journal*, *11*(2), 503–512. https://doi.org/10.1109/jsyst.2015.2438442

[32]. Legg, P. A., Buckley, O., Goldsmith, M., & Creese, S. (2016). *Caught in the act of an insider attack: detection and assessment of insider threat*. 1–6. https://doi.org/10.1109/ths.2015.7446229

[33]. Li, D., Yang, L., Zhang, H., Wang, X., Ma, L., & Xiao, J. (2021). Image-Based Insider Threat

Detection via Geometric Transformation. *Security and Communication Networks*, *2021*, 1–15. https://doi.org/10.1155/2021/1777536

[34]. Lin, L., Zhong, S., Jia, C., & Chen, K. (2017). Insider threat detection based on deep belief network feature representation. *Proceedings - 2017 International Conference on Green Informatics, ICGI 2017*, 54–59. https://doi.org/10.1109/ICGI.2017.37

[35]. Liu, J., Zhang, J., Du, C., & Wang, D. (2023). MUEBA: A Multi-model System for Insider Threat Detection. In Y. Xu, H. Yan, H. Teng, J. Cai, & J. Li (Eds.), *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 13655 LNCS* (pp. 296–310). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-20096-0_23

[36]. Liu, L., De Vel, O., Han, Q. L., Zhang, J., Xiang, Y., & Liu Olivier Y.; Han, Qing-Long; Zhang, Jun; Xiang, Yang, L. de V. (2018). Detecting and Preventing Cyber Insider Threats: A Survey. *IEEE Communications Surveys & Tutorials*, *20*(2), 1397–1417. https://doi.org/10.1109/comst.2018.2800740

[37]. Lu, J., & Wong, R. K. (2019). Insider Threat Detection with Long Short-Term Memory. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3290688.3290692

[38]. Ma, Q., & Rastogi, N. (2020). DANTE: Predicting insider threat using LSTM on system logs. *Proceedings - 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020*, 1151–1156. https://doi.org/10.1109/TrustCom50675.2020.00153

[39]. Meng, F., Lou, F., Fu, Y., & Tian, Z. (2018). Deep learning based attribute classification insider threat detection for data security. *Proceedings - 2018 IEEE 3rd International Conference on Data Science in Cyberspace, DSC 2018*, 576–581. https://doi.org/10.1109/DSC.2018.00092

[40]. Meryem Douzi; Bouabid, El Ouahidi; Mouad, Lemoudden, A. S. (2017). FNC/MobiSPC - A novel approach in detecting intrusions using NSLKDD database and MapReduce programming. *Procedia Computer Science*, *110*(NA), 230–235. https://doi.org/10.1016/j.procs.2017.06.089

[41]. Michael, A., & Eloff, J. H. P. (2019). *A Machine Learning Approach to Detect Insider Threats in Emails Caused by Human Behaviours*. *Haisa*, 34–49.

[42]. Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *BMJ (Clinical Research Ed.)*, *339*, b2535. https://doi.org/10.1136/bmj.b2535

[43]. Nasir, R., Afzal, M., Latif, R., & Iqbal, W. (2021). Behavioral Based Insider Threat Detection Using Deep Learning. *IEEE Access*, *9*, 143266–143274. https://doi.org/10.1109/ACCESS.2021.3118297

[44]. Nasser Al-Mhiqani, M., Ahmed, R., Zainal Abidin, Z. A., & Isnin, S. N. (2021). An Integrated Imbalanced Learning and Deep Neural Network Model for Insider Threat Detection. *International Journal of Advanced Computer Science and Applications*, *12*(1), 573–577. https://doi.org/10.14569/IJACSA.2021.0120166

[45]. Nazir Shushma; Patel, Dilip, S. P. (2017). Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security*, *70*(NA), 436–454. https://doi.org/10.1016/j.cose.2017.06.010

[46]. Neu, C. V., Zorzo, A. F., Orozco, A. M. S., & Michelin, R. A. (2017). An approach for detecting encrypted insider attacks on OpenFlow SDN Networks. *2016 11th International Conference for Internet Technology and Secured Transactions, ICITST 2016*, 210–215. https://doi.org/10.1109/ICITST.2016.7856698

[47]. Okolica, J. S., Peterson, G. L., & Mills, R. F. (2007). Using Author Topic to detect insider threats from email traffic. *Digital Investigation*, *4*(3–4), 158–164. https://doi.org/10.1016/j.diin.2007.10.002

[48]. Pal, P., Chattopadhyay, P., & Swarnkar, M. (2023). Temporal feature aggregation with attention for insider threat detection from activity logs. *Expert Systems with Applications*, 119925. https://doi.org/https://doi.org/10.1016/j.eswa.2023.119925

[49]. Prasad, N. R., Almanza-Garcia, S., & Lu, T. T. (2009). Anomaly detection. *Computers, Materials and Continua*, *14*(1), 1–22. https://doi.org/10.1145/1541880.1541882

[50]. Punithavathani, D. S., Sujatha, K., Jain, J. M., Punithavathani K.; Jain, J. Mark, D. S. S., Punithavathani, D. S., Sujatha, K., & Jain, J. M. (2015). Surveillance of anomaly and misuse in critical networks to counter insider threats using computational intelligence. *Cluster Computing*, *18*(1), 435–451. https://doi.org/10.1007/s10586-014-0403-y

[51]. Rashid, T., Agrafiotis, I., & Nurse, J. R. C. (2016). *A New Take on Detecting Insider Threats*. 47–56. https://doi.org/10.1145/2995959.2995964

[52]. Rose, I., Felts, N., George, A., Miller, E., & Planck, M. (2017). Something Is Better Than Everything: A Distributed Approach to Audit Log Anomaly Detection. *Proceedings - 2017 IEEE Cybersecurity Development Conference, SecDev 2017*, *NA*(NA), 77–82. https://doi.org/10.1109/SecDev.2017.25

[53]. S, A., D, S., & G, P. (2023). Malicious insider threat detection using variation of sampling methods for

anomaly detection in cloud environment. *Computers and Electrical Engineering*, *105*, 108519. https://doi.org/https://doi.org/10.1016/j.compeleceng.2022.108519

[54]. Salem Salvatore J., M. B. S. (2011). A comparison of one-class bag-of-words user behavior modeling techniques for masquerade detection. *Security and Communication Networks*, *5*(8), 863–872. https://doi.org/10.1002/sec.311

[55]. Sanzgiri, A., & Dasgupta, D. (2016). Classification of insider threat detection techniques. *Proceedings of the 11th Annual Cyber and Information Security Research Conference, CISRC 2016*, 5–8. https://doi.org/10.1145/2897795.2897799

[56]. Schuartz, F. C., Fonseca, M., & Munaretto, A. (2020). Improving threat detection in networks using deep learning. In *Annales des Telecommunications/Annals of Telecommunications* (Vol. 75, Issues 3–4, pp. 133–142). https://doi.org/10.1007/s12243-019-00743-5

[57]. Sharma, B., Pokharel, P., & Joshi, B. (2020, July 1). User Behavior Analytics for Anomaly Detection Using LSTM Autoencoder-Insider Threat Detection. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3406601.3406610

[58]. Sheykhkanloo, N. M., & Hall, A. (2020). Insider threat detection using supervised machine learning algorithms on an extremely imbalanced dataset. *International Journal of Cyber Warfare and Terrorism*, *10*(2), 1–26. https://doi.org/10.4018/IJCWT.2020040101

[59]. Singh, A. P., & Sharma, A. (2022). *A systematic literature review on insider threats*. http://arxiv.org/abs/2212.05347

[60]. Singh, M., Mehtre, B. M., Sangeetha, S., & Govindaraju, V. (2023). User Behaviour based Insider Threat Detection using a Hybrid Learning Approach. *Journal of Ambient Intelligence and Humanized Computing*, *14*(4), 4573–4593. https://doi.org/10.1007/s12652-023-04581-1

[61]. Soh, C., Yu, S., Narayanan, A., Duraisamy, S., Chen, L., & Soh Sicheng; Narayanan, Annamalai; Duraisamy, Santhiya; Chen, Lihui, C. Y. (2019). Employee profiling via aspect-based sentiment and network for insider threats detection. *Expert Systems with Applications*, *135*(NA), 351–361. https://doi.org/10.1016/j.eswa.2019.05.043

[62]. Sun, D., & Wang, X. (2021). DeepMIT : A Novel Malicious Insider Threat Detection Framework based on Recurrent Neural Network. *IEEE International Conference on Computer Supported Cooperative Work in Design*, 335–341. https://doi.org/10.1109/CSCWD49262.2021.9437887

[63]. Sun, L., Versteeg, S., Boztas, S., & Rao, A. (2016). *Detecting Anomalous User Behavior Using an Extended Isolation Forest Algorithm: An Enterprise Case Study*. http://arxiv.org/abs/1609.06676

[64]. Tuor, A., Kaplan, S., Hutchinson, B., Nichols, N., & Robinson, S. (2017). Deep learning for unsupervised insider threat detection in structured cybersecurity data streams. *AAAI Workshop - Technical Report*, *WS-17-01*-(2012), 224–234. http://arxiv.org/abs/1710.00811

[65]. Velayudhan, D., Hassan, T., Damiani, E., & Werghi, N. (2023). Recent Advances in Baggage Threat Detection: A Comprehensive and Systematic Survey. *ACM Computing Surveys*, *55*(8), 1–38. https://doi.org/10.1145/3549932

[66]. Walker-Roberts, S., Hammoudeh, M., Dehghantanha, A., & Walker-Roberts Mohammad; Dehghantanha, Ali, S. H. (2018). A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. *IEEE Access*, *6*(NA), 25167–25177. https://doi.org/10.1109/access.2018.2817560

[67]. Wall, A., & Agrafiotis, I. (2021). A bayesian approach to insider threat detection. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *12*(2), 48–84. https://doi.org/10.22667/JOWUA.2021.06.30.048

[68]. Wang, X., Tan, Q., Shi, J., Su, S., & Wang, M. (2018). Insider threat detection using characterizing user behavior. *Proceedings - 2018 IEEE 3rd International Conference on Data Science in Cyberspace, DSC 2018*, 476–482. https://doi.org/10.1109/DSC.2018.00077

[69]. Wei, Y., Chow, K. P., & Yiu, S. M. (2021). Insider threat prediction based on unsupervised anomaly detection scheme for proactive forensic investigation. *Forensic Science International: Digital Investigation*, *38*, 301126. https://doi.org/10.1016/j.fsidi.2021.301126

[70]. Young, W. T., Goldberg, H. G., Memory, A., Sartain, J. F., & Senator, T. E. (2013). Use of domain knowledge to detect insider threats in computer activities. *Proceedings - IEEE CS Security and Privacy Workshops, SPW 2013*, 60–67. https://doi.org/10.1109/SPW.2013.32

[71]. Yuan, F., Cao, Y., Shang, Y., Liu, Y., Tan, J., & Fang, B. (2018). Insider threat detection with deep neural network. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10860 LNCS*, 43–54. https://doi.org/10.1007/978-3-319-93698-7_4

[72]. Yuan, F., Shang, Y., Liu, Y., Cao, Y., & Tan, J. (2020). Data Augmentation for Insider Threat Detection with GAN. *Proceedings - International Conference on Tools with Artificial Intelligence, ICTAI*, *2020-Novem*, 632–638. https://doi.org/10.1109/ICTAI50040.2020.00102

[73]. Yuan, S., & Wu, X. (2021). Deep learning for insider threat detection: Review, challenges and opportunities. *Computers and Security*, *104*, 102221. https://doi.org/10.1016/j.cose.2021.102221

[74]. Yuan, S., Zheng, P., Wu, X., & Li, Q. (2019). Insider Threat Detection via Hierarchical Neural Temporal Point Processes. *Proceedings - 2019 IEEE International Conference on Big Data, Big Data 2019*, 1343–1350. https://doi.org/10.1109/BigData47090.2019.9005589

[75]. Zargar, A., Nowroozi, A., & Jalili, R. (2016). XABA: A zero-knowledge anomaly-based behavioral analysis method to detect insider threats. *13th International ISC Conference on Information Security and Cryptology, ISCISC 2016*, 26–31. https://doi.org/10.1109/ISCISC.2016.7736447

[76]. Zhang, C., Wang, S., Zhan, D., Yu, T., Wang, T., & Yin, M. (2021). Detecting Insider Threat from Behavioral Logs Based on Ensemble and Self-Supervised Learning. *Security and Communication Networks, 2021*. https://doi.org/10.1155/2021/4148441

