International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 12 Issue 9 ǁ September 2024 ǁ PP. 109-117

Insider Threat Detection Techniques: Review of User Behavior Analytics Approach

Olajide O. Ogunbodede[1], Olumide S. Adewale[2], Boniface K. Alese[3], Oluyomi K. Akinyokun[4]

*[*1] Software Engineering Department, Federal University of Technology Akure, Nigeria*
[2]Computer Science Department, Federal University of Technology Akure, Nigeria
[3]Cyber Security Department, Federal University of Technology Akure, Nigeria
[4]Cyber Security Department, Federal University of Technology Akure, Nigeria
Corresponding Author: Olajide O. Ogunbodede ooogunbodede@futa.edu.ng

Abstract

Insider threats pose serious danger to cybersecurity. Insiders possess greater privileges and authorized access to information and resources compared to external attackers, which can result in significant harm to a business if compromised. However, for every malfeasance or benign behavior on a network, digital footprints are often left behind in the user logs. Each abnormal user behavior could be viewed as a potential precursor to a subsequent malicious activity. Detecting insider threats requires thorough analysis of user activity. Authorized users are frequently the primary constituents of the computer network. They frequently perform tremendous activities and tasks on a daily basis. This, in turn, comprises of frequent patterns of regular consumption of diverse resources on the network. Thus, the regular activities and workflow tasks can underline an insightful pattern to map and distinguish user behavior. Researchers are of the opinion that, in order to accurately recognize, detect, and respond to insider threats, a comprehensive analytical approach that incorporates a variety of data sources is preferable. These sources include technological monitoring, behavioral and psychological observations, and profiling. This paper presents a literature review of previous works on insider threat detection based on user behavior analytics.

Keywords: *User Behavior Analytics, Insider Threat detection, CERT datasets.*

Date of Submission: 07-09-2024 Date of acceptance: 21-09-2024

I. INTRODUCTION

Lately, insider threats have been regarded as a critical and recurring problem in the field of information and network security. A successful breach of an organization's security architecture at any time through these threats, often have untold negative impacts on the confidentiality, integrity, and availability (CIA) of data stored in most enterprises' and organizations data warehouses and databases. Thus an organization can lose its competitive edge, incur financial loss through law suits, and could even face bankruptcy as a result of data breaches.

Traditional notions of cybersecurity focuses on external perimeter defense system against attacks that arise from external threats (Al-mhiqani et al., 2020). However, it is becoming increasingly apparent that the greater threat to an organization's security may well lie within, as evidenced in many recent surveys and research findings (Nurse et al., 2014). As a matter of fact, humans have been adjudged as the weakest link in the computer network security chain (Laszka et al., 2013; Rahman et al., 2021; Ogunbodede, 2023). Insider threats refer to individuals or group of individuals that have been given legitimate access right to an organization's internal system, either as an employee, a contractor, or as an ex-employee; and could use this legitimate access to perpetrate malicious acts such as system sabotage, electronic fraud and information theft (Jiang et al., 2019; A. Kim et al., 2020; F. Yuan et al., 2018). That is, the individual with authorized access to information systems poses the biggest threat to security (Roy Sarkar, 2010)

Insider threat detection are often more challenging than the external perimeter breaches that can occur in an enterprise's network and security architecture. This is because the insiders often are familiar with their company's information and network security architecture, both its weaknesses as well its strengths; they can be well equipped to evade and circumvent most work place's internal security mechanisms such as Intrusion Detection Systems (IDS), Honeypots, Firewalls etc. and remain undetected while carrying out their malicious acts.

In addition, threat detection of insiders can be daunting and extremely challenging in that unauthorized steps, abuse and malicious acts by insiders are often woven around the trust factor bestowed on them by their employee or organization (Legg et al, 2015: Colwill, 2015). Authorization to access sensitive information on computers and networks of an organization implies some level of trust (Bishop et al., 2010; Greitzer et al., 2008); thus, the trust factor shields the insider from the external network security framework such as intrusion detection, firewalls, honeypots, and anti-virus. Furthermore, due to the ability to conceal malicious acts, insider threats often are more difficult to detect than most anomaly problems (Colwill, 2009).

Finally, malicious acts by trusted employees or insiders are often concealed inside a large number of normal and benign activities which often can be very difficult to detect. Modeling a user's normal behavior to detect anomalous behavior often serves as key to insider threat detection (S. Yuan & Wu, 2021).

1.1.1 **Background:** Detection Techniques:

Early Insider Threat Research landscape spans across Intrusion Detection, Risk Analysis, Testing and Synthetic Data Generation, and Process Control according to Figure 1 (Raut et al., 2020). Intrusion Detection can be implemented using Anomaly-based and Scenario-based approaches or through deploying honeypots. Risk Analysis often follows the cycle of threat identification, likelihood, assessment, and vulnerability of defense mechanisms deployed. Due to privacy concerns, corporate organizations hardly make their data and audit logs available for public and research consumption. Thus synthetic data generation is increasingly becoming important. Process Control is essential for streamlining and managing efficient incident response (Raut et al., 2020)

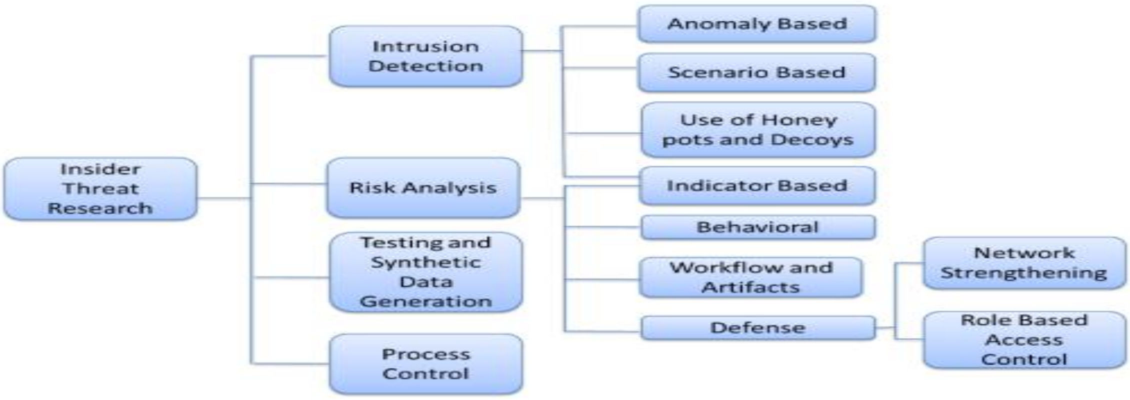


Figure 1. Taxonomy of insider detection methodologies (Sanzgiri & Dasgupta, 2016)

Lately, two main detection methodologies for detecting insider threats, have become prominent according to Figure 2 (Singh et al., 2022). These techniques are: rule-based signature detection and the other, behavior-based anomaly detection. In behavior-based anomaly detection, the system creates a baseline profile of typical system, network, or program activity in behavior-based anomaly detection. Any departure from the predetermined standard is considered malicious (Al-mhiqani et al., 2020). That is, it depends upon the behavior of a particular user or an entity. The second detection methodology is signature-based detection: which recognizes a malicious act that has already been discovered and tagged when its actions correspond with a stored signature or a rule-based protocol that models the system's used behaviors. That is, signature-based detection techniques is often used to detect known attacks or threats.

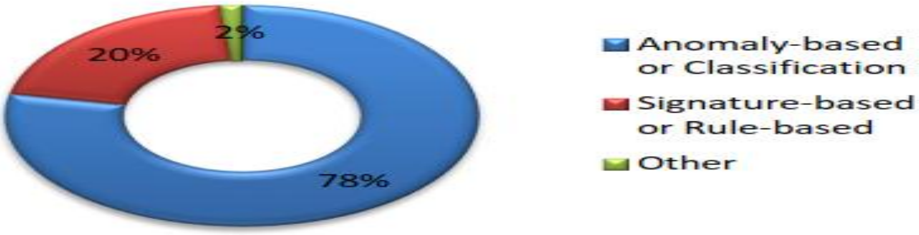


Figure 2 Detection Techniques (Al-mhiqani et al., 2020)

Early works of insider threat detection often aim at user command records. User's command sequence in the UNIX system is used as the analysis object; the probability of occurrence of adjacent command patterns are calculated, including the matching degree between new commands and historical records, respectively, to identify malicious behaviors (C. Zhang et al., 2021). Subsequently, system audit logs were integrated as the analysis tool for detecting insider threats. Consequently, Patcha and Park (Patcha & Park, 2007) aim to detect insider threats in the system audit log and later attribute the difficulty of insider threat detection to the complex data relationship, the difficulty of attack modeling, and the dynamic change of user behaviors.

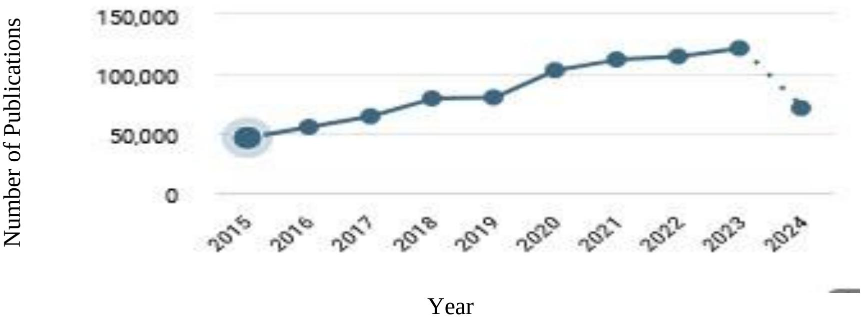


Figure. 3 The trend of security research for the user behavior analytics

Figure 3 above shows the trend of research and publications in user behavior analytics across diverse disciplines starting from the year, 2015. This shows that there has been continuous growth in research interest in analyzing user behavior to back up predictions in cybersecurity and others.

1.1.2 User Behavior Analytics

Numerous academic fields, including psychology, sociology, economics, linguistics, marketing, and computer science, have studied human behavior (Roman et al., 2013). Analyzing user activity is key for detecting insider threats (Alshehri et al., 2023). Often, real users are frequently the primary constituents of the computer network. They frequently perform tremendous activities and tasks on a daily basis. This, in turn, comprises of frequent patterns of regular consumption of diverse resources on the network. Thus, the regular activities and workflow tasks can underline an insightful pattern to map and distinguish user behavior Two types of user behavior usually manifest in an organizational setup: malicious and non-malicious. Insider threats are defined as malicious user behavior (Singh et al., 2022).

Researchers are of the opinion that a comprehensive analysis approach that incorporates a diverse set of data sources from technological monitoring profiling to behavioral and psychological observations is more effective in accurate recognition, detection and response to insider threats (Alahmadi et al., 2014; Legg et al., 2015; Nurse et al., 2014)

According to (Saminathan et al., 2023), User Behavior analytics (UBA) is regarded as a security analysis approach that examines how users behave on networks and systems. This method is used to identify user behavior that is malicious. Deep learning and machine learning algorithms are the cornerstones of this kind of approach and implementation. With UBA, a user's typical behavior is defined as a baseline; if an activity deviates from the baseline, an alert is created. In addition, UBA has been described as the subset and process for the detection of Cybersecurity threats, attacks, and monetary frauds. UBA works on the methods of analyzing the behavior of humans using statistical analysis and algorithms for the detection of Cybersecurity attacks (Alshehri et al., 2023).

System and network logs actively record changes as well as the current state of IT systems and servers. Audit logs mainly involves system logon/logoff, file access, device usage, HTTP access, mail sending and receiving records. Logs assist system administrators in monitoring activities and events, planning for outages and performance issues, and detecting abnormalities in the network (Ma & Rastogi, 2020). Since the information that can be mined from system and network logs is detailed and follows a time sequence, they can reveal information that points towards the possibility of intrusions, abnormal activities, and data theft. The state-of-the-art seems to be still driven by forensics analysis after an attack, rather than technologies that prevent, detect, and deter insider attack. Log analysis remains the state-of-the art in insider attack detection, after a breach has been discovered (Salem et al., 2008). Data for user behavior analysis often falls into two categories: structured data e.g. number and symbol, and unstructured data e.g., text, image and sound (M. Zhang et al., 2015).

Figure 4 below shows the typical basic flow of the user behavior analytics in inside threat detection. Every activity of the user on the company's system or network is archived and stored. Activities ranging from external device used, emails sent, the login and logoff executed, websites visited, file logs accessed, and psychometric data of a user during normal working hours and off periods are archived.

It is important to recognize that during their daily activity, every individual has a unique behavior for every action they take on a system. For example, a user's behavior within the system is affected by how they move the mouse, click or type keystrokes on the keyboard, navigate web pages, etc. (Lu & Wong, 2019; Saminathan et al., 2023).

An indication of anomaly behavior that gives more exposure to insider threats can be detected when the user behavior does not match the expected and usual behavior (Nasir et al., 2021). However, as valuable as capturing user behavior can be, it is pertinent to note that in cyberspace, user behavior is complicated and non-linear (S. Yuan & Wu, 2021). Information about user behavior is difficult and inefficient to gather with manually created features.

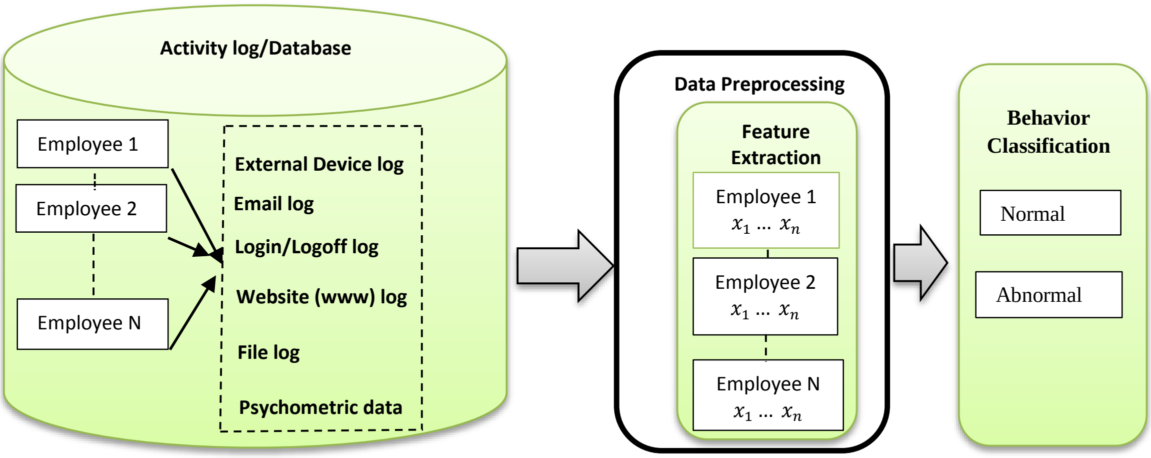


Figure 4 User Behavior Analytics Process in Insider Threat

II. Literature Review

This section presents the reviews and surveys of articles on user behavior analytics as a precursor to detecting malicious insider threat attacks. Sources of these literature include: IEEE Xplore Digital Library, ScienceDirect, SpringerLink, ACM Digital Library, Google Scholar etc. Liu et al, 2023 proposes MUEBA, a multi-modal user entity behavior analytics system for spatiotemporal analysis, which combines individual historical analysis and group behavior analysis for insider threat detection. Attention-based Long Short Term Memory (LSTM) is used to increase the model's sensitivity to abnormal activities using historical analysis. isolation Forest (iForest) algorithm is used for attribute selection and iTree construction. Similarly, Lv and others (Lv et al., 2018) propose an Across-Domain Anomaly Detection (ADAD) model using the iForest algorithm to identify anomalies behaviors among peers. The objective is to address the challenges in detecting insider threats that can have significant implications for situations such as national security, financial stability, and individual privacy.

Similarly, Musili and colleagues (Musili et al, 2017), propose an hybrid framework that combines behavioral variation analysis with technical techniques to provide a real-time mitigation solution for insider threats, with emphasis on detecting, preventing, and responding to these threats. The framework incorporates behavioral variation analysis to detect anomalies in insider activities. Through analyzing the behavioral patterns of individuals within the organization, the system can identify deviations from normal behavior that may indicate insider threats. Patel and the rest (Patel et al., 2017), propose insider attack mitigation technique using hybrid security framework on Vehicular Ad Hoc Networks (VANETs) using a hybrid security framework that combines ID-based and signature-based authentication. The paper includes the implementation of behavioral analysis to detect anomalies in the behavior of vehicles, which can indicate potential insider threats.

Also, Sriram and others (Sriram et al, 2015) propose an Hybrid Protocol to Secure the Cloud from Insider Threats by using enhanced neural network-based user profiling to analyze user behavior patterns, and classify users as malicious or genuine based on predefined thresholds. Thus enhancing the system's ability to detect insider threats.

Furthermore, Tao et al, 2022 proposes an effective insider threat detection approach based on Back Propagation Neural Network (BPNN). A combination of Variational Autoencoder (VAE) that models normal user behavior and Back Propagation Neural Network (BPNN) to identify abnormal user behavior accurately. In their paper, Sharma et al, 2020 proposes user behavior modeling for anomaly detection using Long Short Term (LSTM)

Autoencoder for insider threat detection. The paper uses an unsupervised approach to model user behavior thus discovering anomalous behavior.

In their paper, Zhang and others (Zhang et al., 2018) introduce a deep learning model on integrated and normalized behavior logs to comprehensively learn both normal and abnormal behavior patterns of insiders, creating optimal representations of their behavior features. Similarly, Zhang and colleagues (Zhang et al., 2021) in their paper, considered the application of deep learning over traditional methods which often relies on manual extraction of user behaviors to detect and mitigate insider threats. Traditional methods, they claim, often struggle to model user behaviors over extended periods, hindering accurate threat detection thus necessitating innovative detection strategies such as self-supervised learning and ensemble learning.

Furthermore, Ganapathi and Sharfudeen (Ganapathi & Sharfudeen, 2022) in their research, focuse on identifying unauthorized activities by the insider in the cloud by analyzing user behavior, specifically through web search activities. With this, it would be possible to differentiate between genuine users and malicious users based on their online behavior. Similarly, Nikolai and Wang (Nikolai & Wang, 2016) opines that several traditional approaches for addressing insider attacks in data exfiltration are reactive and not predictive in nature. Thus, they propose a system for detecting malicious insider data theft in IaaS cloud environments, using a system profiling approach for detecting abnormal login activity and data transfers from IaaS cloud computing nodes, hosting tenant virtual machines.

In their paper, Goldberg and others (Goldberg et al., 2016), introduce PRODIGAL, a tool for detecting potential insider threat in computer usage as an ensemble technique. The technique combines results from various detectors to identify anomalous user-days based on real computer usage data. Multiple anomaly detection algorithms were combined to generate a comprehensive assessment of user behavior. In addition, Ma and Rastogi (Ma & Rastogi, 2020) proposes DANTE, a novel approach that uses system logs by various users in an organization, combined with specialized recurrent neural network (RNN) model to analyze sequences of actions recorded in the system logs.

Furthermore, Nasir and colleagues (Nasir et al., 2021) propose a user analytics approach method for detecting insider threats. They categorize user activities as either normal or malicious, which is essential for identifying potential threats from within the organization. This behavioral analysis forms the foundation of their detection approach. Similarly, Le and Zincir-Heywood (Le & Zincir-Heywood, 2021), in their research, utilize advanced data analysis techniques to identify patterns of behavior that may indicate insider threats. User activity logs and other relevant data were analysed to detect anomalies that deviate from normal behavior patterns. As a result of lack of flexibility and adaptability in previous methods responding effectively to sudden changes in user behavior, Amuda and others (Amuda et al., 2022) propose a model designed to adapt to changing patterns in structured data streams. Thus enhancing the detection of malicious insider activities by analyzing user behavior more effectively.

Furthermore, Singh et al, 2020 propose a behavior based detection approach that analyses user behavior within an organization to detect malicious insider threats, rather than relying entirely on predefined rules or signatures. In their subsequent paper, Singh and colleagues (Singh et al., 2022) propose an enhanced insider threat detection method based on user behavior analysis that leads to fewer false positives, faster threat detection, and significantly higher classifier accuracy. Lopez and Sartipi (Lopez & Sartipi, 2020), propose detecting insider threats using Long Short Term Memory (LSTM) neural networks using analysis of user behaviors captured in electronic logs. The study looks at these behaviors in an effort to provide a more efficient way to identify abnormalities that might point to insider threats.

Nepal and Joshi (Nepal & Joshi, 2021) focuse on identifying anomalous activities from user log data to detect insider threats by using a Gated Recurrent Unit (GRU) based Autoencoder to model user behavior and detect anomalies. Lu and Wong (Lu & Wong, 2019) also propose using Long Short Term Memory (LSTM) neural networks because of its sequence prediction capabilities, to analyze historical user behavior by examining daily online activities. Thus, establishing a baseline of normal behavior. The system can more efficiently detect variations that might point to malevolent activity if it knows what each user's average usage is.

Finally, Junhong and colleagues (J. Kim et al., 2019), propose insider threat detection based on user behavior modeling and anomaly detection algorithms. Using user log data, the researchers created datasets containing weekly email communication histories, daily activity summaries, and email content topic distributions. To find malicious activity, they used a variety of anomaly detection methods. And, Tian and the rest (Tian et al., 2020), propose an insider threat detection method based on an attention-LSTM that models normal user behavior and indicates anomalies as malicious behavior. This method combines deep learning and Dempster-Shafer Theory (DST) for insider threat detection with an advanced approach aimed at identifying potential threats posed by individuals within an organization.

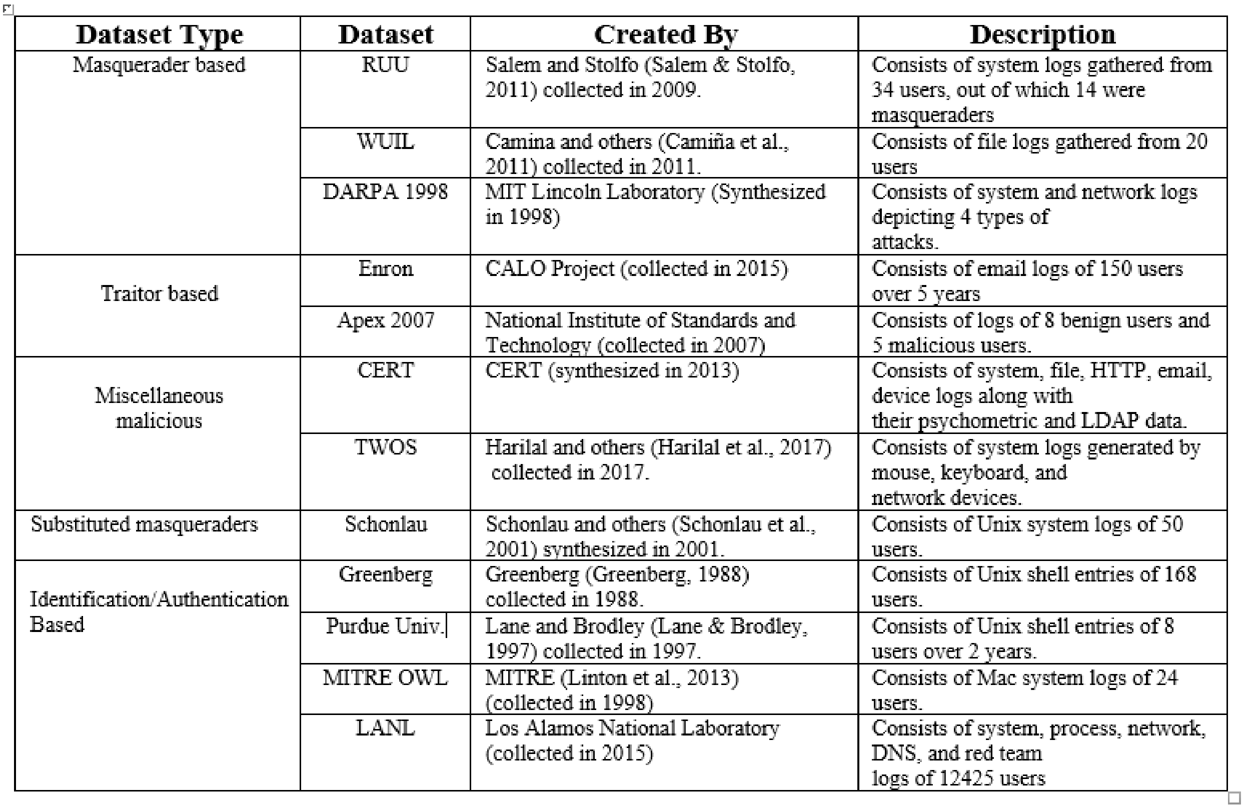
III. DATASET USED

Insider threats are about the actions of human beings, not machines. Since insider threats primarily pertain to human behavior and not otherwise, detection strategies will unavoidably integrate social science methodologies. Datasets are integral part of insider threat detection. Thus this data must contain a thorough description of human behavior in the controlled environment in order to be of any use.

A significant impediment to insider threat research and detection is the lack of data to analyze it (Glasser & Lindauer, 2013). These real data are log files containing private user information, and organizations often refuse to give researchers access to them in order to safeguard their users and assets (Sarhan & Altwaijry, 2023). Nevertheless, under certain regulations, an organization might agree to grant restricted access to the researchers after the private and confidential aspects of the data have been anonymized. This problem makes it challenging for the researchers to carry out their research. To overcome this challenge, researchers find synthetic data preferable.

Homoliak and colleagues (Homoliak et al., 2019), in their survey, outline case studies of incidents of insider threat and existing datasets gathered from laboratory experiments and the real world. They present existing datasets gathered from laboratory experiments and the real world and further group commonly used eleven datasets into five categories: masquerader-based, traitor-based, substituted masqueraders, identification/authentication-based, and miscellaneous malicious (Raut et al., 2020; S. Yuan & Wu, 2021).

Table 1. Insider Threat Detection Datasets (Raut et al., 2020)



Dataset Type	Dataset	Created By	Description
Masquerader based	RUU	Salem and Stolfo (Salem & Stolfo, 2011) collected in 2009.	Consists of system logs gathered from 34 users, out of which 14 were masqueraders
	WUIL	Camina and others (Camiña et al., 2011) collected in 2011.	Consists of file logs gathered from 20 users
	DARPA 1998	MIT Lincoln Laboratory (Synthesized in 1998)	Consists of system and network logs depicting 4 types of attacks.
Traitor based	Enron	CALO Project (collected in 2015)	Consists of email logs of 150 users over 5 years
	Apex 2007	National Institute of Standards and Technology (collected in 2007)	Consists of logs of 8 benign users and 5 malicious users.
Miscellaneous malicious	CERT	CERT (synthesized in 2013)	Consists of system, file, HTTP, email, device logs along with their psychometric and LDAP data.
	TWOS	Harilal and others (Harilal et al., 2017) collected in 2017.	Consists of system logs generated by mouse, keyboard, and network devices.
Substituted masqueraders	Schonlau	Schonlau and others (Schonlau et al., 2001) synthesized in 2001.	Consists of Unix system logs of 50 users.
Identification/Authentication Based	Greenberg	Greenberg (Greenberg, 1988) collected in 1988.	Consists of Unix shell entries of 168 users.
	Purdue Univ.	Lane and Brodley (Lane & Brodley, 1997) collected in 1997.	Consists of Unix shell entries of 8 users over 2 years.
	MITRE OWL	MITRE (Linton et al., 2013) (collected in 1998)	Consists of Mac system logs of 24 users.
	LANL	Los Alamos National Laboratory (collected in 2015)	Consists of system, process, network, DNS, and red team logs of 12425 users

Furthermore, Raut and others (Raut et al., 2020) expanded this to twelve according to Table 1 which summarizes the basic information of the datasets. However, the CERT datasets stand out as being the most widely used by researchers for insider threat detection over the past decade (Sarhan & Altwaijry, 2023). The CERT dataset is a collection of artificial datasets produced by the Community Emergency Response Team (CERT) at Carnegie Mellon University (CMU) for the purpose of validating insider-threat detection techniques (J. Kim et al., 2019).

Table 2: Statistics of CERT r4.2 and r6.2 datasets (Raut et al., 2020)

Version	Employees	Insiders	Activities	Malicious activities
r4.2	1000	70	32,770,227	7323
r6.2	2500	5	135,117,169	470

There are several chronological releases of the CERT insider threat dataset: 1, r2, r3.1, r3.2, r4.1, r4.2, r5.1, r5.2, r6.1, and r6.2 (Raut et al., 2020). However, the most used versions are r4.2 and r6.2. Meanwhile, the most widely used out of the two is the r4.2 data set. It is a dense needle because it contains an unusually large number of insider threats and anomalies compared to the other data sets by CERT (Bulow & Scherman, 2018). The CERT dataset (r4.2) contains behavior data for 1000 users over a period of a year and a half according to Table 2. It has 32,770,222 events from 1000 normal and abnormal users. Deliberately, experts injected 7323 malicious insider instances. On the other hand, r6.2 datasets is referred to as "sparse" dataset that contains 5 insiders and 3995 normal users.

CERT dataset consists of five log files that record the computer-based activities for all employees in a simulated organization: (logon.csv, email.csv, http.csv, file.csv, device.csv). Table 3 lists the activity types in each log file. For each activity, it also contains related descriptions. For example, the activity type "Send Internal Email" includes time, sender, receivers, subject, and content information.

Table 3: Activity Types of CERT Log Files (S. Yuan & Wu, 2021)

Files	Operation Types
logon.csv	Weekday Logon (employee logs on a computer on a weekday at work hours)
	After-hour Weekday Logon (employee logs on a computer on a weekday after work hours)
	Weekend Logon (employees logs on at weekends)
	Logoff (employee logs off a computer)
email.csv	Send Internal Email (employee sends an internal email)
	Send External Email (employee sends an external email)
	View Internal Email (employee views an internal email)
	View external Email (employee views an external email)
http.csv	WWW Visit (employee visits a website)
	WWW Download (employee downloads files from a website)
	WWW Upload (employee uploads files to a website)
device.csv	Weekday Device Connect (employee connects a device on a weekday at work hours)
	After-hour Weekday Device Connect (employee connects a device on a weekday after hours)
	Weekend Device Connect (employee connects a device at weekends)
	Disconnect Device (employee disconnects a device)
file.csv	Open doc/jpg/txt/zip File (employee opens a doc/jpg/txt/zip file)
	Copy doc/jpg/txt/zip File (employee copies a doc/jpg/txt/zip file)
	Write doc/jpg/txt/zip File (employee writes a doc/jpg/txt/zip file)
	Delete doc/jpg/txt/zip File (employee deletes a doc/jpg/txt/zip file)

IV. CONCLUSION

In this brief review paper, we have reviewed various research publications that treated the detection of insider threats based solely on user behavior analysis from log files. The most often used datasets have been highlighted. It is assumed that the log files are immune and shielded from external tampering and manipulation from the malicious insider itself. Insider threats are one of the most challenging threats in cyber security and the main concern of most enterprises, irrespective of size. Although, it is almost impossible to eradicate malfeasance behavior by employees who have been given authorized access to critical information assets, early detection of threats will be helpful for organizations and governments. The use of behavioral modeling techniques of malicious acts can also be adopted as one of the techniques to mitigate insider threats. In addition, the potential resources that the combination of behavioral economics, psychology, and game theory has to offer can be further explored to enhance the early detection and deter malicious acts by trusted insiders. These fields offer more insights into the decision making processes of self-interested agents under risk and uncertainty. Such perceptions can be explored and used as mitigation and deterrence strategies against potential malicious acts by trusted individuals within an establishment.

V. FUTURE RESEARCH DIRECTIONS

Based on this research, we have presented the combination of user insider threat detection techniques and user behavior analytics for insider threats in cyber security. Probable research directions would be to model insider threat behavior of the user and employee within an organization. However, such behavior are known to vary from scenarios to scenarios.

REFERENCES

[1]. Al-mhiqani, M. N., Ahmad, R., Abidin, Z. Z., & Yassin, W. (2020). A-review-of-insider-threat-detection-Classification-machine-learning-techniques-datasets-open-challenges-and-recommendations2020Applied-Sciences-SwitzerlandOpen-Access.pdf. Applied Sciences, 10(15), 5208.

[2]. Alahmadi, B. A., Legg, P. A., & Nurse, J. R. C. (2014). Using Internet Activity Profiling for Insider-Threat Detection.

[3]. Alshehri, A., Khan, N., Alowayr, A., & Alghamdi, M. Y. (2023). Cyberattack Detection Framework Using Machine Learning and User Behavior Analytics. Computer Systems Science and Engineering, 44(2), 1679–1689. https://doi.org/10.32604/csse.2023.026526

[4]. Amuda, O. K., Akinyemi, B. O., Sanni, M. L., & Aderounmu, G. A. (2022). A Predictive User Behaviour Analytic Model for Insider Threats in Cyberspace. International Journal of Communication Networks and Information Security, 14(1), 150–159. https://doi.org/10.17762/ijcnis.v14i1.5208

[5]. Bishop, M., Engle, S., Frincke, D. A., Gates, C., Greitzer, F. L., Peisert, S., & Whalen, S. (2010). A Risk Management Approach to the "Insider Threat." 115–137. https://doi.org/10.1007/978-1-4419-7133-3_6

[6]. Bulow, J., & Scherman, M. (2018). Insider Threat detection using Isolation Forest. 1–67. http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8952203&fileOId=8952292

[7]. Colwill, C. (2009). Human factors in information security: The insider threat - Who can you trust these days? Information Security Technical Report, 14(4), 186–196. https://doi.org/10.1016/j.istr.2010.04.004

[8]. Ganapathi, P., & Sharfudeen, A. (2022). Detection of Malicious Insider in Cloud Environment based on Behavior Analysis. April. https://doi.org/10.1201/9781003302384-1

[9]. Glasser, J., & Lindauer, B. (2013). Bridging the Gap : A Pragmatic Approach to Generating Insider Threat Data. https://doi.org/10.1109/SPW.2013.37

[10]. Goldberg, H. G., Young, W. T., Memory, A., & Senator, T. E. (2016). Explaining and Aggregating Anomalies to Detect Insider Threats. https://doi.org/10.1109/HICSS.2016.344

[11]. Greitzer, F. L., Moore, A. P., Cappelli, D. M., Andrews, D. H., Carroll, L. A., & Hull, T. D. (2008). Combating the insider cyber threat. IEEE Security and Privacy, 6(1), 61–64. https://doi.org/10.1109/MSP.2008.8

[12]. Homoliak, I., Toffalini, F., Guarnizo, J., & Elovici, Y. (2019). Insight Into Insiders and IT : A Survey of Insider Threat Taxonomies , Analysis , Modeling , and Countermeasures. 52(2).

[13]. Jiang, W., Tian, Y., Liu, W., Liu, W., Jiang, W., Tian, Y., Liu, W., Liu, W., Insider, A., Detection, T., Based, M., Jiang, W., Tian, Y., Liu, W., & Liu, W. (2019). An Insider Threat Detection Method Based on User Behavior Analysis To cite this version : HAL Id : hal-02197790 An Insider Threat Detection Method based on User Behavior Analysis.

[14]. 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

[15]. Kim, J., Park, M., Kim, H., Cho, S., & Kang, P. (2019). Insider threat detection based on user behavior modeling and anomaly detection algorithms. Applied Sciences (Switzerland), 9(19). https://doi.org/10.3390/app9194018

[16]. Laszka, A., Johnson, B., Schöttle, P., Grossklags, J., & Böhme, R. (2013). Managing the weakest link: A game-theoretic approach for the mitigation of insider threats. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8134 LNCS(September), 273–290. https://doi.org/10.1007/978-3-642-40203-6_16

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

[18]. Legg, P. A., Buckley, O., Goldsmith, M., & Creese, S. (2015). Automated Insider Threat Detection System using User and Role-based Profile Assessment. October 2020. https://doi.org/10.1109/JSYST.2015.2438442

[19]. Lopez, E., & Sartipi, K. (2020). Detecting the Insider Threat with Long Short Term Memory (LSTM) Neural Networks. http://arxiv.org/abs/2007.11956

[20]. 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

[21]. M. Musili, Stephen, M. Kimwele, R. R. (2017). Hybrid Insider Cyber Security Threats Mitigation Scheme Using ECC and Behavoural Analysis Methodology. Advances in Wireless Communications and Networks, 3(4), 29. https://doi.org/10.11648/j.awcn.20170304.11

[22]. 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

[23]. 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

[24]. Nepal, S., & Joshi, B. (2021). User Behavior Analytics for Insider Threat Detection using Deep Learning. 8914, 232–238.

[25]. Nikolai, J., & Wang, Y. (2016). A System for Detecting Malicious Insider Data Theft in IaaS Cloud Environments A System for Detecting Malicious Insider Data Theft in IaaS Cloud Environments.

[26]. Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. T., & Whitty, M. (2014). Understanding Insider Threat : A Framework for Characterising Attacks. https://doi.org/10.1109/SPW.2014.38

[27]. Ogunbodede, O. O. (2023). Game Theory Classification in Cybersecurity: A Survey. Applied and Computational Engineering, 2(1), 670–678. https://doi.org/10.54254/2755-2721/2/20220644

[28]. Patcha, A., & Park, J. (2007). An overview of anomaly detection techniques : Existing solutions and latest technological trends. 51, 3448–3470. https://doi.org/10.1016/j.comnet.2007.02.001

[29]. Patel, D., Rohokale, V., & Naresh, G. (2017). Insider Attack Mitigation Technique using Hybrid Security Framework on VANETs. May, 195–199.

[30]. Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021). Human Factors in Cybersecurity: A Scoping Review. ACM International Conference Proceeding Series, July. https://doi.org/10.1145/3468784.3468789

[31]. Raut, M., Dhavale, S., Singh, A., & Mehra, A. (2020). Insider threat detection using deep learning: A review. Proceedings of the 3rd International Conference on Intelligent Sustainable Systems, ICISS 2020, 856–863. https://doi.org/10.1109/ICISS49785.2020.9315932

[32]. Roman, P. E., Velásquez, J. D., Palade, V., & Jain, L. C. (2013). Preface. Studies in Computational Intelligence, 452(June 2015). https://doi.org/10.1007/978-3-642-33326-2

[33]. Roy Sarkar, K. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. Information Security Technical Report, 15(3), 112–133. https://doi.org/10.1016/j.istr.2010.11.002

[34]. Salem, M. Ben, Hershkop, S., & Stolfo, S. J. (2008). A Survey of Insider Attack Detection Research. Advances in Information Security, 39(May), 69–70. https://doi.org/10.1007/978-0-387-77322-3_5

[35]. Saminathan, K., Mulka, S. T. R., Damodharan, S., Maheswar, R., & Lorincz, J. (2023). An Artificial Neural Network Autoencoder for Insider Cyber Security Threat Detection. Future Internet, 15(12). https://doi.org/10.3390/fi15120373

[36]. 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

[37]. Sarhan, B. Bin, & Altwaijry, N. (2023). applied sciences Insider Threat Detection Using Machine Learning Approach.

[38]. Singh, M., Mehtre, B., & Sangeetha, S. (2022). User behavior based Insider Threat Detection using a Multi Fuzzy Classifier. In Multimedia Tools and Applications (Vol. 81, Issue 16). https://doi.org/10.1007/s11042-022-12173-y

[39]. Sriram M , Vaibhav Patel , Harishma D, N. L. (2015). Sriram M , Vaibhav Patel , Harishma D , Nachammai Lakshmanan. IEEE International Conference on Cloud Computing in Emerging Markets (CCEM).

[40]. Tian, Z., Shi, W., Tan, Z., Qiu, J., Sun, Y., & Jiang, F. (2020). Deep Learning and Dempster-Shafer Theory Based Insider Threat Detection.

[41]. 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

[42]. 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

[43]. 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

[44]. Zhang, J., Chen, Y., & Ju, A. (2018). Insider threat detection of adaptive optimization DBN for behavior logs. Turkish Journal of Electrical Engineering and Computer Sciences, 26(2), 792–802. https://doi.org/10.3906/elk-1706-163

[45]. Zhang, M., Wang, Y., & Chai, J. (2015). Review of User Behavior Analysis Based on Big Data: Method and Application. Ameii. https://doi.org/10.2991/ameii-15.2015.17