Journal of Advanced Research in Social Sciences and Humanities
Volume 6, Issue 4 (167-174)
DOI: https://dx.doi.org/10.26500/JARSSH-06-2021-0402

Review of insider and insider threat detection in the organizations

Arshiya Subhani [1]*, Iftikhar Alam Khan [2], Anmol Zubair [3]

[1, 2, 3] Bath Spa University, Academic Centre RAK, UAE

Abstract

Aim: The insider threat is a severe issue in cyber security. Insider threats are largely overlooked by most companies. Workers, system administrators, and outside contractors all have access to confidential company data. It is critical for the organization's finances and reputation that such sensitive information is kept secret. If sensitive information were to escape the hands of even a tiny percentage of the authorized workforce, it could cause catastrophic financial losses. Protecting a company from the potentially disastrous actions of its own employees presents a formidable challenge, and identifying and eliminating the insider threat is a crucial part of that. This study aims to determine the types of insider threats that can exist within an organization and the best methods for countering them.

Methodology: Research on the topic of insider danger is summarized in this paper. Insiders (representing types of insiders, motivation, insider access, methods used by insiders, insider profiling, and levels of insiders); Threat Detection Methods (describing methodology, techniques, datasets used to implement various insider threat detection techniques, and different analyzed user behavior); and Insider Threat Analysis (describing the various analyzed behavior of the user) are the three categories into which the research has been sorted.

Findings: Within today's increasingly digitalized businesses, dishonest employees pose a significant risk. Since the global changes in the business environment, insider threats have become a problem for most companies. There has been an increase in the insider threat since 2019, and one primary reason is the widespread adoption of cloud computing and bring-your-own-device policies for remote work.

Implications/Novel Contribution: Future studies are encouraged to improve threat detection methods, evaluate the efficacy of existing methods using a real-world dataset, and adopt a hybrid approach to developing effective models for detecting insider threats.

Keywords: Analyzed behavior of insiders, insider threats, insider threat detection techniques, types of insiders, metric evaluation.

Received: 09 August 2021/ **Accepted:** 13 October 2021 / **Published:** 28 December 2021

INTRODUCTION

Organizations worldwide need help keeping up with the sophisticated hacking methods of cybercriminals due to the rapid pace of technological change. Unfortunately, while many businesses take precautions against hackers on the outside, they often overlook the threat posed by employees. An insider threat is "a person who has the potential to harm an organization for which they have inside knowledge or access," as stated by the author Chan (2019). Employees with access to sensitive information pose a significant risk to an organization because of the "insider threat."

The cost of insider threats is expected to increase by 31%, from $8.76 million in 2018 to $11.45 million in 2020, as reported by a study by Proofpoint (2021). Since humans are the least reliable security mechanism, we are usually to blame when sensitive information is compromised. 85% of data breach incidents are caused by human error, according to research by Stanford University Professor Jeff Hancock and security firm Tessian (Tessian, 2021; Tongkaw, 2019). Some 27% of data breaches and 67% of phishing attacks were caused by the carelessness of insiders, per the ENISA Threat Landscape report 2018 Sfakianakis, Douligeris, Marinos, Lourenço, and Raghimi (2019). Employee carelessness, such as using simple passwords, sharing passwords, not locking devices after use, or connecting to unsecured Wi-Fi, also contributes to the prevalence of insider threat attacks. X-Force found that 60% of active technology threats resulted from malicious insiders, and 40% resulted from employee negligence (Liewtrakul & Kaewbanjong, 2017; Singleton, 2021). Organizations are at risk from malicious insider threats for various reasons, including retaliation against coworkers, conflicts with employees, dissatisfaction with the job or to help family and friends, industrial/IT sabotage, or the pursuit of business advantage (Dawson, 2015; Gelles, 2016).

*Email: arshiya@bathspa.ae

53% of cyber security professionals agree that it is difficult to detect insiders in the cloud, based on the findings of the Insider threat report by cyber security insiders (Cybersecurity, 2021).

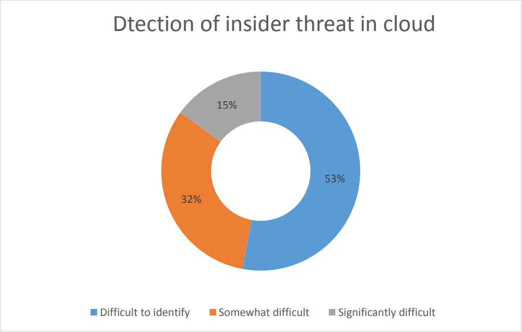

Figure 1. Dtection of insider threat in cloud

To protect important assets, the organizations should be aware of the impact of the insider threat and implement methods to control the threats caused by insiders.

LITERATURE REVIEW

The researches done so far on insider threats are based on three aspects, the first one is insider, the second one is insider threat detection, and the third one is threat analysis. The graphical representation explains the classification of the insider review. Followed by sections that describe the each classification in detail. Description begins with who are insiders, their motivation, types, and their effects and is followed by methods, techniques, and evaluation metrics.

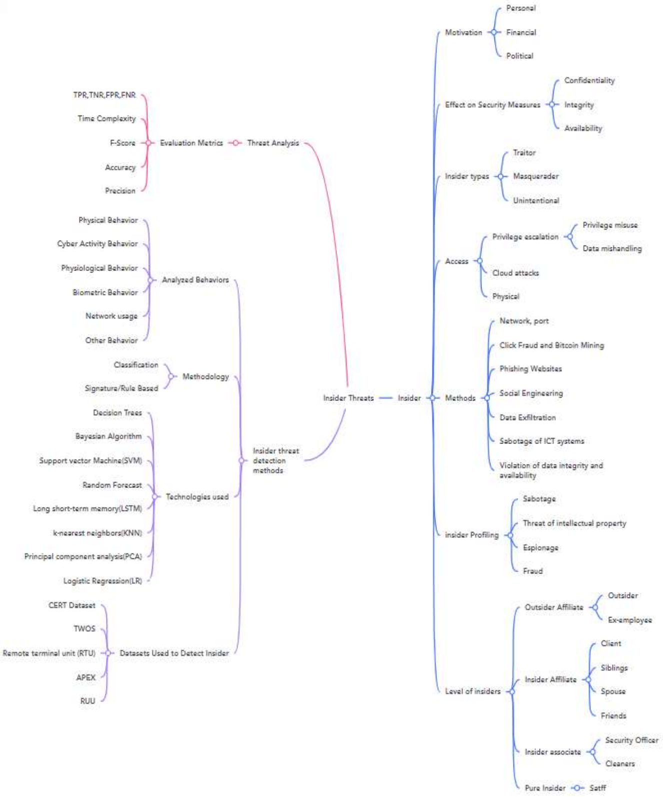

Figure 2. Classifications of insider threats research

Insider

The insiders are the authorized employees who have direct access to the resources, in physical access the insiders directly connect to the network and devices to collect the data or perform an action. The privilege escalation represents a misuse of privilege access or misuse of confidential data. The insiders are classified as masquerade, traitors and unintentional users. Masquerade is the one who accesses the resources pretending as the authorized user. Traitors are the users who have direct access to the resources and perform the actions intentionally. The unintentional users are the ones who perform the actions leading to the threat to the organization without their knowledge. As per the Data Breach investigation report Verizon (2021), the 30% of the attacks are due to mishandling of confidential data. The cloud attacks are made by insiders who have gained access to the organization's cloud.

Motivation

Identifying motivation for the insiders is most important to detect the insiders. According to Cole and Ring (2005), the motivation is classified as financial, political and personal. The report Verizon (2021) states that among the 265 incidents in 2021 the, 80% of the privileged misuse of data is caused by financial motivation. The other motivation of malicious insiders could be different political views of staff that may lead to harm the organization. The third motivation could be personal. It could be a particular employee's personal opinion or blackmailing the employee.

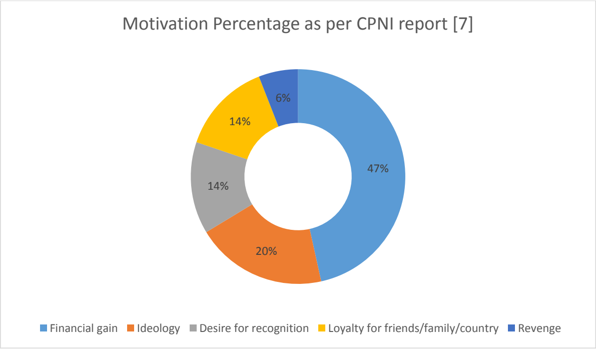

Figure 3. Motivation percentage as per CPNI report (CPNI, 2013)

These numbers show that the organizations should not focus on outsider's malicious attacks but also on insider attacks to strengthen the organization's security.

Insider Profiling

As per the authors in the book- The CERT guide to insider threats (Cappelli, Moore, & Trzeciak, 2012), insider profiling is classified as sabotage, where malicious insider uses the data/devices to sabotage the employee/organization, theft of intellectual property where malicious insider leaks the organization's confidential data, fraud which represents unauthorized access of data/resources by a malicious insider, and espionage revealing the organization's confidential information by a malicious insider for political/military or economic benefits (Cole & Ring, 2005).

Effect on Security Measures

The CIA model describes that confidentiality, integrity and authentication are the three major security measures in any organization. The authentication represents that only the authorized users shall have access to the resources. The malicious insider can get unauthorized access to misuse the resources or alter the information (integrity) and also leak the confidential data. As per the authors in Al-Mhiqani et al. (2018), the malicious insiders have access to organizational resources, have knowledge about the important organizational assets, and also gain the trust of the organization.

Insider Levels

The insider levels are classified (BaMaung, McIlhatton, MacDonald, & Beattie, 2018; Gunasekhar, Rao, & Basu, 2015; Long et al., 2011) as pure insider – employee who has complete access to the organizational resources, insider affiliate-employee who doesn't have complete access to the organizational resources but has complete knowledge about the organizational resources, for example the friend/spouse, insider associate-the one who doesn't have access to the organizational network but still can use the resources like devices for example the cleaners of the organization, and outside affiliate the one who gets access to the organizational resources illegally.

INSIDER THREAT DETECTION METHODS

This section describes the techniques, datasets used to detect the insider, and use of analyzed behavior of the malicious insider.

Techniques Used to Detect The Insider Threat

The most common insider threats are data exfiltration, data integrity and availability, and sabotage (Liu, De Vel, Han, Zhang, & Xiang, 2018). According to the research Farahmand and Spafford (2013), perceived risk and benefit of insiders are inversely proportional, also proposed a model to identify the perceptions of risks involved and the characteristics of insiders and also how to identify insiders. The near-miss management system was proposed by author Oktem (2003) to identify and provide security from unintentional insider threats. The near-miss process (Oktem, 2003) consists of eight steps. First one is to understand the definition of unintentional insider threat and identify the near-miss. The second step is to record the identified near-miss to organize and better understand the impact of the threat. The third step is to prioritize the incident of threat that occurred. The fourth step is to distribute the identified insider threat report to identify the cause of the threat. The fifth step is to identify the root cause of the threat and also to detect vulnerability if it exists. The sixth step is to provide the solutions to the identified root cause of the threat. The seventh step is to disseminate the solutions to the ones who were affected by the threat, and the eighth step is tracking the solutions and recording them for future identification of similar threats. The near-miss concept is a bottom-top strategy to identify the insider threats.

In previous research, the prediction of insider threats models was developed. As per the research Schultz (2002), multiple indicators such as employee behavior, personality traits were used to predict the insider threats. In contrast, the prediction model proposed in Kandias, Mylonas, Virvilis, Theoharidou, and Gritzalis (2010) uses many factors such as user taxonomy, psychological profiling, real time usage data, and a decision algorithm to identify the insider threats. Some threat detection techniques monitor employee activities to predict the threats. The UNICOS Christoph et al. (1995) proposed a model to create user profiles to count the number of times users access the system at a specified time to detect unusual employee behavior. Several techniques were proposed to model the insider threat behavior. The Bayesian algorithm was used to model a structured method to detect unusual insider behavior using the log files (Ambre & Shekokar, 2015). The one-class SVMS was used in Parveen et al. (2013) to build the insider threat detection model upon the normal streams of unbounded and evolving data using the concept of data stream mining which increases the weighted cost of false negatives and the accuracy of the prediction.

The Behavior Based Access Control (BBAC) method proposed in Mayhew, Atighetchi, Adler, and Greenstadt (2015) uses machine learning algorithms like K-Means++ clustering algorithm, Decision Trees algorithm, and Support Vector Machine algorithms based classifiers to control scalability, to predict the suspicious network data like HTTP requests and TCP connection behavior and also improves scalability and reduce false positives by adding dynamic nodes to the model. The BN modeling method was presented in research Roberts et al. (2016) that uses various detectors and fusion algorithms upon the dataset of users to predict the insider threat, also suggested that previous predictions could be introduced as a new node to the existing model to increase the accuracy of the prediction done by the insider threat detection model. The research in Garfinkel, Beebe, Liu, and Maasberg (2013) uses forensics tools and the approaches like Bulk Data Analysis, Random Sampling, and Automated File System Metadata Extraction to build the local surveillance system to detect unusual employee behavior compared to the co-workers and their earlier work history and also detect the user accounts if it is accessed by an outsider the and generate the report on regular-but-unpredictable basis. The author Yuan et al. (2018) presents a model for insider threat detection developed using a Deep Neural Network, this process uses the Long Short Term memory (LSTM) to learn the unusual user behavior and extracts it into a featured matrix and Convolution Neural Network (CNN) uses this featured matrix to detect the insider threat, the accuracy - 0.09449 is achieved by the experiment done on the dataset in the best case. Many researches were based on machine learning methods, neural networks, clustering, and statistical classification to develop threat detection techniques. Upcoming research requires a detailed understanding of the insider to detect the threat and prevent organizational loss.

Analyzed Behavior

Biometric analysis was done by the researcher in Wang, Tan, Shi, Su, and Wang (2018), describes the mouse movement as a measure of a malicious insider. The various methods like SVM, PNN, decision trees, Bayesian algorithm were used to model the malicious insider behavior. The Chen et al. (2014) uses a similar feature with keystroke biometric to model the behavior of the malicious insider. The cyber activity behavior is described in many research based on the activities like login, email access, etc. The researchers in Nikolai and Wang (2016) provided the k-nearest neighbor to detect the insider in cloud and proposed a solution for data theft in cloud IaaS architecture. The log features of email, files, HTTP , devices were used to detect the insider using machine learning methods (Lo, Buchanan, Griffiths, & Macfarlane, 2018). Psychosocial Behaviors of insiders like tension, agitation, and anxiety were used to develop an information leakage detection system (Lee, Park, Eom, & Chung, 2015). The physical behavior of the user was detected by using the Euclidean distance to identify user's behavior represented in nodes, log details of various resources like email, cameras, websites (Meng, Li, Wang, & Au, 2020). The other behavior of insiders was analyzed by focusing on various features like use of authorized data and transfer of data, keystrokes of a user, use of resources like printer, scanner and USB in (Nithiyanandam, Tamilselvan, Balaji, & Sivaguru, 2012) using a layered defense system proposed on monitoring of data and activity of a user.

Dataset Used

The several parameters like Id, timestamp, date, PC, etc. of HTTP, Email, login/logoff, File and Devices from CERT dataset (Kaggle, 2022) were used in Lo et al. (2018); Böse, Avasarala, Tirthapura, Chung, and Steiner (2017) many research. RUU sensor was used to model the biometric identification of user behavior to detect the insider threat (Song, Salem, Hershkop, & Stolfo, 2013). A gamified competition was modeled to obtain a TWOS dataset of instances of insider threat to monitor the features like keystrokes, mouse clicks, network traffic, email, and log details (Harilal et al., 2017). The APEX data set is used to detect the malicious analyst. A normalization method is used to identify the data's inconsistency and noise that occurs due to malicious analysis behavior (Santos et al., 2011).

Evaluation Metrics

To detect the insider threat, many classification evaluation metrics are used. They are represented in below table.

Table 1: Evaluation metrics

Evaluation Metrics	Description and References
Precision = TP/(TP+FP)	Precision represents a true malicious insider value (Parveen et al., 2013; Nikolai & Wang, 2016)
True Positive Rate TPR = TP/(TP+FN)	It is defined as the fraction of insider threat data on malicious entries that are correctly classified (Lo et al., 2018; Parveen et al., 2013; Nikolai & Wang, 2016)
True Negative Rate TNR = TN/(TN+FP)	TNR represents the ability of the model to correctly identify data without malicious entries of data (Nikolai & Wang, 2016)
False Positive Rate FPR = FP/(FP+TN)	The fraction value is calculated as a number of legitimate insiders marked as malicious to an actual number of legitimate insiders (Parveen et al., 2013, 2013; Wang et al., 2018)

Table 1 Continue...

Evaluation Metrics	Description and References
False Negative Rate FNR = FN/(FN+TP)	False negative indicates the fraction of the missed malicious insiders that are considered as legitimate insiders by the model (Wang et al., 2018)
F-score = 2(Precision.Recall/(Precision+Recall))	The F-score is calculated as a harmonic mean between sensitivity and precision (Wang et al., 2018)
Accuracy = (TN+TP)/(TN+TP+FN+FP)	The accuracy represents the efficiency of the model developed (Lo et al., 2018; Yuan et al., 2018)
Time complexity	The time is taken by the model to complete the task of classification (Mayhew et al., 2015)

Challenges in Detecting Insider Threats

In the real world, most of the organizations ignore insider threats due to ethical or privacy issues in the organization. The most of the existing research done is based on the existing data. Even though the data is collected from the server log, it can only be used later in the offline forensics to detect the insider (Mayhew et al., 2015). It is difficult to apply the models developed on the live data to detect the insider in the organizations. The external tools like firewalls, antivirus software, and threat detection systems can't detect the malicious insiders (Hsieh, Lai, Mao, Kao, & Lee, 2015) as most of the insiders perform malicious activity during working hours. The complexity of the detection of malicious internal also increases due to the encrypted mechanisms used to perform the malicious activities. The other challenge of the existing threat detection method is differentiating the authorized and malicious users.

CONCLUSION

In the current digital era, one of the dangerous threats to organizations is due to the insiders. Most of the organizations are facing issues with insider threats since the global changes in the business environment. Excessive use of cloud and BYOD concepts to work from home was one of the major reason to increase the insider threat since 2019. Various research and studies are held in the field to detect and identify the malicious insider in the organizations based on various factors like log details, time stamps, email usage, server log, keystrokes, and mouse handling. This paper focused on reviewing the concept of insider and insider threat detection. Some of the recommendations for upcoming research are to use the hybrid solution to develop the effective models to detect the insider threats, to enhance threat detection methods, and evaluate the performance of the existing methods using the live dataset.

REFERENCES

Al-Mhiqani, M. N., Ahmad, R., Yassin, W., Hassan, A., Abidin, Z. Z., Ali, N. S., & Abdulkareem, K. H. (2018). Cyber-security incidents: A review cases in cyber-physical systems. *International Journal of Advanced Computer Science and Applications*, *9*(1), 499-508.

Ambre, A., & Shekokar, N. (2015). Insider threat detection using log analysis and event correlation. *Procedia Computer Science*, *45*, 436-445. doi:https://doi.org/10.1016/j.procs.2015.03.175

BaMaung, D., McIlhatton, D., MacDonald, M., & Beattie, R. (2018). The enemy within? The connection between insider threat and terrorism. *Studies in Conflict & Terrorism*, *41*(2), 133-150. doi:https://doi.org/10.1080/1057610X.2016.1249776

Böse, B., Avasarala, B., Tirthapura, S., Chung, Y.-Y., & Steiner, D. (2017). Detecting insider threats using radish: A system for real-time anomaly detection in heterogeneous data streams. *IEEE Systems Journal*, *11*(2), 471-482. doi:https://doi.org/10.1109/JSYST.2016.2558507

Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT guide to insider threats: How to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud)*. Boston, MA: Addison-Wesley.

Chan, M. Y. (2019). A study on the establishing alternative security system in transition order. *International Journal of Technology and Engineering Studies*, *5*(5), 157–162. doi:https://dx.doi.org/10.20469/ijtes.5.10003-5

Chen, X.-J., Shi, J.-Q., Xu, R., Yiu, S., Fang, B.-X., & Xu, F. (2014). PAITS: Detecting masquerader via short-lived interventional mouse dynamics. In *International Conference on Applications and Techniques in Information Security,* Berlin, Heidelberg. doi:https://doi.org/10.1007/978-3-662-45670-5_22

Christoph, G. G., Jackson, K. A., Neuman, M. C., Siciliano, C. L., Simmonds, D. D., Stallings, C. A., & Thompson, J. L. (1995). UNICORN: Misuse detection for unicos^{TM}. In *Supercomputing'95: Proceedings of the 1995 ACM/IEEE Conference on Supercomputing,* San Diego, CA. doi:https://doi.org/10.1109/SUPERC.1995.241777

Cole, E., & Ring, S. (2005). *Insider threat: Protecting the enterprise from sabotage, spying, and theft*. Amsterdam, Netherlands: Elsevier.

CPNI. (2013). *Insider data collection study* (Tech. Rep.). London, UK: CPNI.

Cybersecurity. (2021). *Insider thereat report.* Retrieved from https://bit.ly/3uVoHSE

Dawson, M. (2015). *New threats and countermeasures in digital crime and cyber terrorism*. Hershey, PA: IGI Global.

Farahmand, F., & Spafford, E. H. (2013). Understanding insiders: An analysis of risk-taking behavior. *Information Systems Frontiers*, *15*(1), 5-15. doi:https://doi.org/10.1007/s10796-010-9265-x

Garfinkel, S. L., Beebe, N., Liu, L., & Maasberg, M. (2013). Detecting threatening insiders with lightweight media forensics. In *International Conference on Technologies for Homeland Security (HST),* Waltham, MA. doi:https://doi.org/10.1109/THS.2013.6698981

Gelles, M. G. (2016). *Insider threat: Prevention, detection, mitigation, and deterrence*. Oxford, UK: Butterworth-Heinemann.

Gunasekhar, T., Rao, K. T., & Basu, M. T. (2015). Understanding insider attack problem and scope in cloud. In *International Conference on Circuits, Power and Computing Technologies,* Nagercoil, India. doi:https://doi.org/10.1109/ICCPCT.2015.7159380

Harilal, A., Toffalini, F., Castellanos, J., Guarnizo, J., Homoliak, I., & Ochoa, M. (2017). Twos: A dataset of malicious insider threat behavior based on a gamified competition. In *Proceedings of the 2017 International Workshop on Managing Insider Security Threats,* Dallas, TX. doi:https://doi.org/10.1145/3139923.3139929

Hsieh, C.-H., Lai, C.-M., Mao, C.-H., Kao, T.-C., & Lee, K.-C. (2015). AD2: Anomaly detection on active directory log data for insider threat monitoring. In *International Carnahan Conference on Security Technology (ICCST),* Taipei, Taiwan. doi:https://doi.org/10.1109/CCST.2015.7389698

Kaggle. (2022). *CERT insider threat.* Retrieved from https://bit.ly/3J5lc18

Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., & Gritzalis, D. (2010). An insider threat prediction model. In *International Conference on Trust, Privacy and Security in Digital Business,* Berlin, Heidelberg.

Lee, H.-J., Park, M.-W., Eom, J.-H., & Chung, T.-M. (2015). New approach for detecting leakage of internal information; using emotional recognition technology. *KSII Transactions on Internet and Information Systems (TIIS)*, *9*(11), 4662-4679. doi:https://doi.org/10.3837/tiis.2015.11.023

Liewtrakul, P., & Kaewbanjong, K. (2017). A semantic web service retrieval approach that combines semantic matching with quality of service matching. *Journal of ICT, Design, Engineering and Technological Science*, *1*(2), 42–47. doi:https://doi.org/10.33150/jitdets-1.2.3

Liu, L., De Vel, O., Han, Q.-L., Zhang, J., & Xiang, Y. (2018). Detecting and preventing cyber insider threats: A survey. *IEEE Communications Surveys & Tutorials*, *20*(2), 1397-1417. doi:https://doi.org/10.1109/COMST.2018.2800740

Lo, O., Buchanan, W. J., Griffiths, P., & Macfarlane, R. (2018). Distance measurement methods for improved insider threat detection. *Security and Communication Networks*, *2018*, 1-8.

Long, J., Wiles, J., Rogers, R., Drake, P., Green, R. J., Kipper, G., ... Schroader, A. (2011). *Techno security's guide to managing risks for it managers, auditors, and investigators*. Amsterdam, Netherlands: Elsevier.

Mayhew, M., Atighetchi, M., Adler, A., & Greenstadt, R. (2015). Use of machine learning in big data analytics for insider threat detection. In *Military Communications Conference,* Tampa, FL. doi:https://doi.org/10.1109/MILCOM.2015.7357562

Meng, W., Li, W., Wang, Y., & Au, M. H. (2020). Detecting insider attacks in medical cyber–physical networks based on behavioral profiling. *Future Generation Computer Systems*, *108*, 1258-1266. doi:https://doi.org/10.1016/j.future.2018.06.007

Nikolai, J., & Wang, Y. (2016). A system for detecting malicious insider data theft in IaaS cloud environments. In *Global Communications Conference (GLOBECOM)* Washington, DC. doi:https://doi.org/10.1109/GLOCOM.2016.7841554

Nithiyanandam, C., Tamilselvan, D., Balaji, S., & Sivaguru, V. (2012). Advanced framework of defense system for prevetion of insider's malicious behaviors. In *International Conference on Recent Trends in Information Technology,* Chennai, India. doi:https://doi.org/10.1109/ICRTIT.2012.6206788

Oktem, U. G. (2003). *Near-miss: A tool for integrated safety, health, environmental and security management* (Tech. Rep.). New York, NY: AIChE.

Parveen, P., Mcdaniel, N., Weger, Z., Evans, J., Thuraisingham, B., Hamlen, K., & Khan, L. (2013). Evolving insider threat detection stream mining perspective. *International Journal on Artificial Intelligence Tools*, *22*(5), 1-24.

Proofpoint. (2021). *2020 cost of insider threat global report* (Tech. Rep.). Sunnyvale, CA: Proofpoint.

Roberts, S. C., Holodnak, J. T., Nguyen, T., Yuditskaya, S., Milosavljevic, M., & Streilein, W. W. (2016). A model-based approach to predicting the performance of insider threat detection systems. In *Security and Privacy Workshops (SPW),* San Jose, CA. doi:https://doi.org/10.1109/SPW.2016.14

Santos, E., Nguyen, H., Yu, F., Kim, K. J., Li, D., Wilkinson, J. T., . . . Clark, B. (2011). Intelligence analyses and the insider threat. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, *42*(2), 331-347. doi:https://doi.org/10.1109/TSMCA.2011.2162500

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, *21*(6), 526-531. doi:https://doi.org/10.1016/S0167-4048(02)01009-X

Sfakianakis, A., Douligeris, C., Marinos, L., Lourenço, M., & Raghimi, O. (2019). *ENISA threat landscape report 2018.15 top cyberthreats and trends* (Tech. Rep.). Athens, Greece: ENISA.

Singleton, C. (2021). *X-force threat intelligence index* (Tech. Rep.). Armonk, NY: IBM.

Song, Y., Salem, M. B., Hershkop, S., & Stolfo, S. J. (2013). System level user behavior biometrics using fisher features and gaussian mixture models. In *Security and Privacy Workshops,* San Francisco, CA. doi:https://doi.org/10.1109/SPW.2013.33

Tessian. (2021). *The psychology of human error - tessian* (Tech. Rep.). Broadgate Circle, UK: Tessian.

Tongkaw, A. (2019). Software defined network, the design, technique, and internet of things defined in campus network. *International Journal of Technology and Engineering Studies*, *5*(3), 80–89. doi:https://dx.doi.org/10.20469/ijtes.5.10002-3

Verizon. (2021). *Data breach investigations report.* Retrieved from https://bit.ly/3x05txQ

Wang, X., Tan, Q., Shi, J., Su, S., & Wang, M. (2018). Insider threat detection using characterizing user behavior. In *In Ieee Third International Conference on Data Science in Cyberspace (DSC),* Guangzhou, China. doi:https://doi.org/10.1109/DSC.2018.00077

Yuan, F., Cao, Y., Shang, Y., Liu, Y., Tan, J., & Fang, B. (2018). Insider threat detection with deep neural network. In *International Conference on Computational Science,* Cham, UK. doi:https://doi.org/10.1007/978-3-319-93698-7_4