PRIVACY AND SECURITY OF INSIDER THREATS IN CLOUD - CURRENT TRENDS, DETECTION AND CHALLENGES - A REVIEW

Deepthi Bolukonda
Research Scholar, Dept. of Computer Science and Engineering
Jawaharlal Nehru Technological University, Hyderabad, India, 500085
deepthiraya@gmail.com
Assistant Professor, Dept. of Computer Science and Engineering
Chaitanya Bharathi Institute of Technology
Gandipet, Hyderabad, India, 500075
Vijaya Kumari Gunta
Professor, Dept. of Computer Science and Engineering
Jawaharlal Nehru Technological University,Hyderabad, India, 500085
vijayakumari.gunta@gmail.com

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 analyzed 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. The study also includes a classification of current trends in insider risk. This review can provide as a starting point for new researchers and a standard for scholars who are proposing new insider threat detection methodologies.

Keywords: Insider Threat; Insider Threat Trends; Insider Threat detection

Introduction

Insider threat is the term used to describe the risk posed to the security, resources, or data of an organization by those who have been granted permission to use these resources, such as employees, partners, or contractors. Insiders may perform acts that threaten the organization's security intentionally or accidentally, such as stealing confidential information, disrupting operations, or merely making mistakes. Because insiders frequently have deep knowledge of the organization's vulnerabilities and resources, insider threats are particularly harmful and facilitating their ability to conduct attacks or avoid identify (Greitzer Deborah A., 2010).

Insider risks can take many different shapes, including physical harm, espionage, sabotage, theft, and cybercrime. In more depth, violence can refer to actions that provoke hostility or abuse, whereas espionage can be defined as the use of covert methods to gather information for purposes of military, political, or economic benefit. Sabotage entails deliberate measures to undermine an organization's physical and digital infrastructure, whereas theft can involve the unauthoritative seizure of cash or intellectual property. Theft, espionage, violence, and sabotage related to technology, devices, or the internet are the final types of cyber actions. While purposeful threats are malicious activities that use technological means to interrupt ordinary corporate operations, get protected information, or carry out an attack strategy, unintentional risks can also result from the non-malicious exposure of IT infrastructure (CISA, 2022).

An insider threat typically aims to use their access to private data or systems to carry out harmful acts including stealing confidential information, financial data, or intellectual property, destroying systems or processes, or engaging in fraud. The insider danger may occasionally be driven by selfish interests, retaliation, ideology, or just plain carelessness. A serious insider threat may have negative effects on the organization's finances, reputation, and legal standing. Therefore, in order to identify, stop, and reduce the danger of insider threats, organisations need to put in place adequate security measures.

Researchers have been working to discover an effective solution to attacks being carried out by the insider threat as a result of the rise in insider threat incidents (Axelrad et al., 2013; J Liu et al., 2023; M Singh et al., 2023). Therefore, it is anticipated that the suggested solutions will significantly lessen its harmful effects, decrease false alarms, and raise its detection rate.

Finding a solution to the insider threat led to a flood of insider threat analysis in the literature. Despite the fact that researchers have made significant efforts (Axelrad et al., 2013; Michael and Eloff, 2019; Pal et al., 2023; Prasad et al., 2009; Sharma et al., 2020), a permanent solution to the insider danger has not yet materialised.

Insider danger has been the subject of prior systematic reviews in the literature. But the primary problem with those earlier analyses was that they largely focused on insider danger in the healthcare sector and certain other particular fields.

In this study, we propose to do an exhaustive, systematic assessment of all analyses done on insider threat activities, including its assault model, types, detection, and environment protection.

The goal of this literature review is to provide an in-depth knowledge of the attack mode, organisational structure, and behaviour of various insider threats, to comprehend the causes of insider threats' growth, and to see what insider threat experts and researchers are saying and doing to put a limit in their excessive behaviour. The following are the paper's main contributions:

1. We looked at the criteria used to assess insider threat attacks and detection systems.

2. For a future investigation of the structure of insider threats, we tabulated and summarised all research datasets that were available.

3. We give a thorough analysis of insider threat detection techniques in the literature.

Literature Review:

Insider threats and their identification were thoroughly reviewed by the authors (AP Singh and Sharma, 2022) who also highlighted the key categories and techniques for minimizing insider threat attacks.

(Al-mhiqani et al., 2020) provide a classification of modern insider types, access, level, motivation, insider profiling, effect security properties, and methods used by attackers to conduct attacks as well as analysedbehaviours, machine-learning techniques, dataset, detection methodology, and evaluation metrics. The number of publications in each database source taken into consideration for the systematic review is shown.

(Kim et al., 2020) conducted research on how insider threat data should be gathered and used in the industry to detect insider risks in the Internet of Things (IoT) environment. They reviewed insider threat detection methodologies.

S Yuan and Wu's poll from 2021 regarding the use of deep learning strategies for detecting insider threats, a discussion of recent advancements and probable future directions in insider threat detection using deep learning, as well as an application of this technology to the detection of anomalies and the identification and categorization of difficulties.

The authors of the paper (Kim et al., 2019) examined the various insider threats based on insider characteristics and insider activities, explored the sensors that make it possible to detect insider threats in an automated way, and examined the public datasets available for research. By doing so, they gave readers a systematic understanding of the prior literature that addresses the problems with insider threat detection.

A systematic evaluation of insider threat detection was undertaken by Walker-Roberts et al. (2018), but the review's scope was limited to insider threats to critical infrastructures in the healthcare industry.

2017's (Nazir Shushma; Patel, Dilip) thorough study on modelling, simulation, and associated methods that have been employed to evaluate the susceptibility of the supervisory control and data acquisition (SCADA) system to cyberattacks was made available.

A distributed, automated detection system with a centralized repository was proposed in the research effort by Rose et al. (2017).

(Jiang et al., 2016) conducted a survey on the machine-learning approaches that can be used to a variety of computer security areas, such as intrusion detection systems, software security, security policy management, malware identification, and malware mitigation.

Insider threat detection methods are further broken down into nine classes in a study (Sanzgiri and Dasgupta, 2016): anomaly-based approaches, role-based access control, scenario-based techniques, decoy documents and honeypot techniques, risk analysis using psychological factors, risk analysis using workflow, improving network defense, improving defense by access control, and process control to deter insiders.

The research by (Gheyas Ali E. et al., 2016) indicated that the dataset-game theory approach (GTA), feature-insider's online behavior’s, and algorithm-graph algorithm were the three most prominent research topics in the area.

Table 1:Related Surveys on Insider Threat

S. No.	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	(NazirShushma; 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. METHODOLOGY

The research methodology section outlines the procedures used to review the previous publications on insider threat attack and detection systems. We also describe how the current studies were chosen using a set of inclusion and exclusion criteria.

3.1 Study Protocol and Phases

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

3.2 Sources for Search and Data

To find relevant material on insider threat and defence strategies, several databases were searched. The publications underwent thorough examination using several methods to identify primary research. As indicated in Table 2, the research methodology used for this article involved searching through pertinent papers from numerous academic databases, including ACM Digital Library, IEEE Xplore, Science Direct, Springer, Taylor & Francis, Web of Science, and Wiley Online Library.

Table 2: Search Database Sources

S. No.	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

IV. INSIDER THREAT DETECTION TECHNIQUE SYNTHESES

Table 3: Syntheses of Insider Threat Detection Techniques

S/N	Reference	Techniques	Problem Addressed	Results/Findings	Limitation	Dataset
1	(Haq et al., 2022)	Long Short-Term Memorymodels 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.	Enron corps, CERT

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 largescale deployments	CERT
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	CERT
4	(Li et al., 2021)	The techniques used in this method include feature extraction, image conversion, and a modified unsupervised anomaly detection algorithm.	It addresses the problem of an approach that converts the unsupervised anomaly detection problem into a supervised image classification problem, thereby reducing the complexity of the detection process.	The results show that the proposed method outperforms existing methods in terms of detection accuracy and false alarm rate	The proposed method may not be suitable for detecting advanced insider threats that involve sophisticated attack techniques.	NSLKDD
5	(Nasir et al., 2021)	This paper used LSTM-Autoencoder as the algorithm	The paper addresses the problem of insider threat detection in networked systems of companies and	The paper addresses the problem of insider threat detection in networked systems of companies and	The performance is dependent on the quality and quantity of the data used for training and	CERT

			government agencies.	government agencies.	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.	CERT
7	(Ma and Rastogi, 2020)	The paper Proposed a novel 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.	The paper addresses the problem of insider threat detection in information communicatio n technology to successfully detect only known types of anomalies from the log entries	The proposed model achieved a 93% prediction accuracy rate.	Relies on system logs to detect insider behaviour, and the proposed approach may require significant computationa l resources to process large amounts of system logs	Enron corps
8	(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 results show that the model can achieved 90% accuracy rate	The paper does not provide information on the scalability of the proposed platform	CERT

9	(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 auto encoder on the non-anomalous dataset and then using it to define the threshold to separate the outliers from the normal data points	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	NSLKDD
10	(J Jiang et al., 2019)	Random Forest	Graph Convolutional Networks.	94.5% and 83.3% were recorded for accuracy and recall.	94.5% and 83.3% were recorded for accuracy and recall.	CERT
11	(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 singledomain behavior, 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.	NSLKDD

V. CHALLENGES AND FUTURE SCOPE

Despite the fact that there have been numerous researchers and solutions developed over the years, the average global cost of insider threat incidents has increased over the last two years, rising from $8.76 million in 2018 to $15.4 million in 2022. Negligent insiders account for 56% of all incidents and cost an average of $484,931 per incident (Ponemon Institute, 2022). This is not a result of a lack of answers, but rather of obstacles that stop such solutions from working effectively, such as technological advancements, the sheer number of devices that are connected, and the lack of expertise among employers and employees.
An efficient method of detecting insider threats should be able to do so in real time while also ensuring that false alarms don't lower the rate of detection accuracy.

Machine learning can undoubtedly help with insider threat detection, but the effectiveness of each method will ultimately depend on the quantity, quality, and design of the dataset used in the experiment.

When all logs are taken into account and the danger level is continuously updated, any detection technique should be able to produce results that are comparable even when the environment changes. To provide predictive capabilities of insider threat identification, this detection system should make use of a method of dynamic and reliable behavior forecasting analysis combined with intelligent machine learning.

Preventing employees from bringing in or using private devices to access information within the company is one of the most effective measures against insider threat. Real-time monitoring should be used in combination with this.

VI.CONCLUSIONS

In order to help beginner researchers interested in insider danger, we give in this study a thorough evaluation of insider threat detection mechanisms from 2010 to 2023.

Techniques for detecting insider threats have been looked at, researched, and surveyed for this reason. Future study is anticipated to determine the most practical and efficient detection method to counter 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 insiderthreat 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-insiderthreats

[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).: RNN Autoencoder 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., &NurZincir-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 RoleBased 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

[33].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