REFERENCES

Alajlan, A. M., & Almasri, M. M. (2022). Malicious behavior detection in cloud using self- optimized dynamic kernel convolutional neural network. *Transactions on Emerging Telecommunications Technologies*, *33*(5), e4449.

Al-Mhiqani, M. N., Ahmad, R., Abidin, Z. Z., Abdulkareem, K. H., Mohammed, M. A., Gupta, D., & Shankar, K. (2022). A new intelligent multilayer framework for insider threat detection. *Computers & Electrical Engineering*, *97*, 107597.

Al-Mhiqani, M. N., Ahmed, R., Abidin, Z. Z., & Isnin, S. N. (2021). An integrated imbalanced learning and deep neural network model for insider threat detection. *International Journal of Advanced Computer Science and Applications*, *12*(1).

Al-Mhiqani, M. N., Alsboui, T., Al-Shehari, T., Abdulkareem, K. H., Ahmad, R., & Mohammed, M. A. (2024). Insider threat detection in cyber-physical systems: a systematic literature review. *Computers & Electrical Engineering*, *119*, 109489. https://doi.org/10.1016/j.compeleceng.2024.109489

Al-Shehari, T. A., Rosaci, D., Al-Razgan, M., Alfakih, T., Kadrie, M., Afzal, H., & Nawaz, R. (2024a). Enhancing insider threat detection in imbalanced cybersecurity settings using the density-based local outlier factor algorithm. *IEEE Access*, *12*, 34820-34834.

Al-Shehari, T., & Alsowail, R. A. (2021). An insider data leakage detection using one-hot encoding, synthetic minority oversampling and machine learning techniques. *Entropy*, *23*(10), 1258.

Al-Shehari, T., & Alsowail, R. A. (2023). Random resampling algorithms for addressing the imbalanced dataset classes in insider threat detection. *International Journal of Information Security*, *22*(3), 611-629.

Al-Shehari, T., Al-Razgan, M., Alfakih, T., Alsowail, R. A., & Pandiaraj, S. (2023). Insider threat detection model using anomaly-based isolation forest algorithm. *IEEE Access*, *11*, 118170-118185.

Al-Shehari, T., Kadrie, M., Al-Mhiqani, M. N., Alfakih, T., Alsalman, H., Uddin, M., ... & Dandoush, A. (2024b). Comparative evaluation of data imbalance addressing techniques for CNN-based insider threat detection. *Scientific Reports*, *14*(1), 24715.

Alshehri, A. (2022). Relational deep learning detection with multi-sequence representation for insider threats. *International Journal of Advanced Computer Science and Applications*, *13*(5).

AlSlaiman, M., Salman, M. I., Saleh, M. M., & Wang, B. (2023). Enhancing false negative and positive rates for efficient insider threat detection. *Computers & Security*, *126*, 103066.

Alzaabi, F. R., & Mehmood, A. (2024). A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. *IEEE Access*, *12*, 30907-30927.

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.

Anakath, A. S., Kannadasan, R., Joseph, N. P., Boominathan, P., & Sreekanth, G. R. (2022). Insider Attack Detection Using Deep Belief Neural Network in Cloud Computing. *Computer Systems Science & Engineering*, *41*(2).

Andrean, A., Jayabalan, M., & Thiruchelvam, V. (2020). Keystroke dynamics based user authentication using deep multilayer perceptron. *International Journal of Machine Learning and Computing*, *10*(1), 134-139.

Arsh, A., Kar, N., Das, S., & Deb, S. (2024). Multiple approaches towards authentication using keystroke dynamics. *Procedia Computer Science*, *235*, 2609-2618.

Asha, S., Shanmugapriya, D., & Padmavathi, G. (2023). Malicious insider threat detection using variation of sampling methods for anomaly detection in cloud environment. *Computers and Electrical Engineering*, *105*, 108519.

Aversano, L., Bernardi, M. L., Cimitile, M., & Pecori, R. (2021). Continuous authentication using deep neural networks ensemble on keystroke dynamics. *PeerJ Computer Science*, *7*, e525.

Babu, B. M., & Bhanu, M. S. (2015). Prevention of insider attacks by integrating behavior analysis with risk based access control model to protect cloud. *Procedia Computer Science*, *54*, 157-166.

Baynath, P., Soyjaudah, K. S., & Khan, M. H. M. (2018, December). Machine learning algorithm on keystroke dynamics pattern. In *2018 IEEE Conference on Systems, Process and Control (ICSPC)* (pp. 11-16). IEEE.

Bellovin, S. M. (2008). The insider attack problem nature and scope. In *Insider Attack and Cyber Security: Beyond the Hacker* (pp. 1-4). Boston, MA: Springer US.

Besnaci, S., Hafidi, M., & Lamia, M. (2023, March). Dealing with extremly unbalanced data and detecting insider threats with deep neural networks. In *2023 International Conference on Advances in Electronics, Control and Communication Systems (ICAECCS)* (pp. 1-6). IEEE.

Bhana, B., & Flowerday, S. (2020). Passphrase and keystroke dynamics authentication: Usable security. *Computers & Security*, *96*, 101925.

Bishop, M., Engle, S., Peisert, S., Whalen, S., & Gates, C. (2009, January). Case studies of an insider framework. In *2009 42nd Hawaii International Conference on System Sciences* (pp. 1-10). IEEE.

Budžys, A., Kurasova, O., & Medvedev, V. (2025). Integrating deep learning and data fusion for advanced keystroke dynamics authentication. *Computer Standards & Interfaces*, *92*, 103931.

Bunkhumpornpat, C., & Subpaiboonkit, S. (2013, September). Safe level graph for synthetic minority over-sampling techniques. In *2013 13th International Symposium on Communications and Information Technologies (ISCIT)* (pp. 570-575). IEEE.

Carnegie Mellon University. (2023, May 30). *Insider Threat test Dataset*. Figshare. https://kilthub.cmu.edu/articles/dataset/Insider_Threat_Test_Dataset/12841247

Çevik, N., Akleylek, S., & Koç, K. Y. (2021, September). Keystroke dynamics based authentication system. In *2021 6th International Conference on Computer Science and Engineering (UBMK)* (pp. 644-649). IEEE.

Chang, H. C., Li, J., Wu, C. S., & Stamp, M. (2022). Machine learning and deep learning for fixed-text keystroke dynamics. In *Artificial intelligence for cybersecurity* (pp. 309-329). Cham: Springer International Publishing.

Chatalic, A., Schreuder, N., Rosasco, L., & Rudi, A. (2022, June). Nyström kernel mean embeddings. In *International Conference on Machine Learning* (pp. 3006-3024). PMLR.

Chattopadhyay, P., Wang, L., & Tan, Y. P. (2018). Scenario-based insider threat detection from cyber activities. *IEEE Transactions on Computational Social Systems*, *5*(3), 660-675.

Chen, Z., Cai, H., Jiang, L., Zou, W., Zhu, W., & Fei, X. (2021, May). Keystroke dynamics based user authentication and its application in online examination. In *2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD)* (pp. 649-654). IEEE.

Chintalapudi, S. R., Garapati, S. S. V., Kumar, A. D. P., & Ram, K. S. S. (2020). A Machine Learning Approach for User Identification using Keystroke Dynamics. *Journal of emerging technologies and innovative research*, *7*, 521-526.

Cleghorn, L. (2013). Network Defense Methodology: A comparison of defense in depth and defense in breadth. *Journal of Information Security*, *04*(03), 144–149. https://doi.org/10.4236/jis.2013.43017

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

Diop, A., Emad, N., Winter, T., & Hilia, M. (2019). Design of an ensemble learning Behavior Anomaly Detection Framework. *International Journal of Computer and Information Engineering*, *13(10)*.

Dittman, D. J., Khoshgoftaar, T. M., & Napolitano, A. (2014, November). Selecting the appropriate data sampling approach for imbalanced and high-dimensional bioinformatics datasets. In *2014 IEEE International Conference on Bioinformatics and Bioengineering* (pp. 304-310). IEEE.

EGUAVOEN, V. O., & NWELIH, E. (2025). HSML-ITD: HYBRID SUPERVISED MACHINE LEARNING FRAMEWORK FOR INSIDER THREAT DETECTION. *Quantum Journal of Engineering, Science and Technology*, *6*(1), 100-110.

Elhassan, T., & Aljurf, M. (2016). Classification of imbalance data using tomek link (t-link) combined with random under-sampling (rus) as a data reduction method. *Global J Technol Optim S*, *1*, 2016.

El-Kenawy, E. S. M., Mirjalili, S., Abdelhamid, A. A., Ibrahim, A., Khodadadi, N., & Eid, M. M. (2022). Meta-heuristic optimization and keystroke dynamics for authentication of smartphone users. *Mathematics*, *10*(16), 2912.

Eltoukhy, M. M., Gaber, T., Almazroi, A. A., & Mohamed, M. F. (2024). ONE3A: one-against-all authentication model for smartphone using GAN network and optimization techniques. *PeerJ Computer Science*, *10*, e2001.

Fei, K., Zhou, J., Zhou, Y., Gu, X., Fan, H., Li, B., ... & Chen, Y. (2025). LaAeb: A comprehensive log-text analysis based approach for insider threat detection. *Computers & Security*, *148*, 104126.

Ferreira, P., Le, D. C., & Zincir-Heywood, N. (2019, October). Exploring feature normalization and temporal information for machine learning based insider threat detection. In *2019 15th International Conference on Network and Service Management (CNSM)* (pp. 1-7). IEEE.

Folino, G., Otranto Godano, C., & Pisani, F. S. (2023). An ensemble-based framework for user behaviour anomaly detection and classification for cybersecurity. *The Journal of Supercomputing*, *79*(11), 11660-11683.

Fujiwara, K., Huang, Y., Hori, K., Nishioji, K., Kobayashi, M., Kamaguchi, M., & Kano, M. (2020). Over-and under-sampling approach for extremely imbalanced and small minority data problem in health record analysis. *Frontiers in public health*, *8*, 178.

Gao, P., Zhang, H., Wang, M., Yang, W., Wei, X., Lv, Z., & Ma, Z. (2025). Deep temporal graph infomax for imbalanced insider threat detection. *Journal of Computer Information Systems*, *65*(1), 108-118.

Garba, N., Rakshit, S., Mang, C. D., & Vajjhala, N. R. (2021, April). An email content-based insider threat detection model using anomaly detection algorithms. In *Proceedings of the International Conference on Innovative Computing & Communication (ICICC)* (pp. 1-5).

Gayathri, R. G., Sajjanhar, A., & Xiang, Y. (2024). Hybrid deep learning model using spcagan augmentation for insider threat analysis. *Expert Systems with Applications*, *249*, 123533.

Gayathri, R. G., Sajjanhar, A., Xiang, Y., & Ma, X. (2021, October). Anomaly detection for scenario-based insider activities using CGAN augmented data. In *2021 IEEE 20th international conference on trust, security and privacy in computing and communications (TrustCom)* (pp. 718-725). IEEE.

Giura, P., & Wang, W. (2012, December). A context-based detection framework for advanced persistent threats. In *2012 International Conference on Cyber Security* (pp. 69-74). IEEE.

Gosain, A., & Sardana, S. (2017, September). Handling class imbalance problem using oversampling techniques: A review. In *2017 international conference on advances in computing, communications and informatics (ICACCI)* (pp. 79-85). IEEE.

Gu, Y., Wang, Y., Wang, M., Pan, Z., Hu, Z., Liu, Z., ... & Dong, M. (2021). Secure user authentication leveraging keystroke dynamics via Wi-Fi sensing. *IEEE Transactions on Industrial Informatics*, *18*(4), 2784-2795.

Hasanin, T., & Khoshgoftaar, T. (2018, July). The effects of random undersampling with simulated class imbalance for big data. In *2018 IEEE international conference on information reuse and integration (IRI)* (pp. 70-79). IEEE.

He, H., Bai, Y., Garcia, E. A., & Li, S. (2008, June). ADASYN: Adaptive synthetic sampling approach for imbalanced learning. In *2008 IEEE international joint conference on neural networks (IEEE world congress on computational intelligence)* (pp. 1322-1328). IEEE.

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 (CSUR)*, *52*(2), 1-40.

Huang, A., Gao, S., Chen, J., Xu, L., & Nathan, A. (2020). High security user authentication enabled by piezoelectric keystroke dynamics and machine learning. *IEEE Sensors Journal*, *20*(21), 13037-13046.

Hunker, J., & Probst, C. W. (2011). Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, *2*(1), 4-27.

IBM. (2024). *Cost of a data breach 2024*, IBM. https://www.ibm.com/reports/data-breach

Jaafar, F., Nicolescu, G., & Richard, C. (2016, August). A systematic approach for privilege escalation prevention. In *2016 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)* (pp. 101-108). IEEE.

Jadhav, C., Kulkami, S., Shelar, S., Shinde, K., & Dharwadkar, N. V. (2017, February). Biometrie authentication using keystroke dynamics. In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)* (pp. 870-875). IEEE.

Jaiswal, A., Dwivedi, P., & Dewang, R. K. (2024). Handling imbalance dataset issue in insider threat detection using machine learning methods. *Computers and Electrical Engineering*, *120*, 109726.

Janjua, F., Masood, A., Abbas, H., & Rashid, I. (2020). Handling insider threat through supervised machine learning techniques. *Procedia Computer Science*, *177*, 64-71.

Janssen, C. *What is data exfiltration? - definition from Techopedia*. Techopedia. (2013, January 9). https://www.techopedia.com/definition/14682/data-exfiltration

Jiang, J., Chen, J., Gu, T., Choo, K. K. R., Liu, C., Yu, M., ... & Mohapatra, P. (2019, November). Anomaly detection with graph convolutional networks for insider threat and fraud detection. In *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)* (pp. 109-114). IEEE.

Jiang, W., Tian, Y., Liu, W., & Liu, W. (2018). An insider threat detection method based on user behavior analysis. In *IFIP advances in information and communication technology* (pp. 421–429). https://doi.org/10.1007/978-3-030-00828-4_43

Jindal, R., & Singh, I. (2022). Detecting malicious transactions in database using hybrid metaheuristic clustering and frequent sequential pattern mining. *Cluster Computing*, *25*(6), 3937-3959.

Kamatchi, K., & Uma, E. (2024). Securing the edge: privacy-preserving federated learning for insider threats in IoT networks. *The Journal of Supercomputing*, *81*(1).

Khan, N., J. Houghton, R., & Sharples, S. (2022). Understanding factors that influence unintentional insider threat: a framework to counteract unintentional risks. *Cognition, Technology & Work*, *24*(3), 393-421.

Killourhy, K. S., & Maxion, R. A. (2009, June). Comparing anomaly-detection algorithms for keystroke dynamics. In *2009 IEEE/IFIP international conference on dependable systems & networks* (pp. 125-134). IEEE.

Kim, D. I., Lee, S., & Shin, J. S. (2020). A new feature scoring method in keystroke dynamics-based user authentications. *IEEE Access*, *8*, 27901-27914.

Krishnamoorthy, S., Rueda, L., Saad, S., & Elmiligi, H. (2018, May). Identification of user behavioral biometrics for authentication using keystroke dynamics and machine learning. In *Proceedings of the 2018 2nd international conference on biometric engineering and applications* (pp. 50-57).

Lamiche, I., Bin, G., Jing, Y., Yu, Z., & Hadid, A. (2019). A continuous smartphone authentication method based on gait patterns and keystroke dynamics. *Journal of Ambient Intelligence and Humanized Computing*, *10*, 4417-4430.

Le, D. C., & Zincir-Heywood, A. N. (2018, May). Evaluating insider threat detection workflow using supervised and unsupervised learning. In *2018 IEEE Security and Privacy Workshops (SPW)* (pp. 270-275). IEEE.

Le, D. C., & Zincir-Heywood, N. (2020, June). Exploring adversarial properties of insider threat detection. In *2020 IEEE Conference on Communications and Network Security (CNS)* (pp. 1-9). IEEE.

Le, D. C., & Zincir-Heywood, N. (2021). Anomaly detection for insider threats using unsupervised ensembles. *IEEE Transactions on Network and Service Management*, *18*(2), 1152–1164. https://doi.org/10.1109/tnsm.2021.3071928

Lin, K. B., Weng, W., Lai, R. K., & Lu, P. (2014, August). Imbalance data classification algorithm based on SVM and clustering function. In *2014 9th International Conference on Computer Science & Education* (pp. 544-548). IEEE.

Lindauer, B. (2020). Insider Threat Test Dataset. *Carnegie Mellon University*. *Dataset*. https://doi.org/10.1184/R1/12841247.v1

Liu, J., Zhang, J., Du, C., & Wang, D. (2022, December). Mueba: A multi-model system for insider threat detection. In *International Conference on Machine Learning for Cyber Security* (pp. 296-310). Cham: Springer Nature Switzerland.

Liu, L., De Vel, O., Chen, C., Zhang, J., & Xiang, Y. (2018, November). Anomaly-based insider threat detection using deep autoencoders. In *2018 IEEE international conference on data mining workshops (ICDMW)* (pp. 39-48). IEEE.

Maciejewski, T., & Stefanowski, J. (2011, April). Local neighbourhood extension of SMOTE for mining imbalanced data. In *2011 IEEE symposium on computational intelligence and data mining (CIDM)* (pp. 104-111). IEEE.

Maharjan, P., Shrestha, K., Bhatta, T., Cho, H., Park, C., Salauddin, M., ... & Park, J. Y. (2021). Keystroke dynamics based hybrid nanogenerators for biometric authentication and identification using artificial intelligence. *Advanced Science*, *8*(15), 2100711.

Mamidanna, S. K., Reddy, C. R. K., & Gujju, A. (2022, January). Detecting an insider threat and analysis of XGBoost using hyperparameter tuning. In *2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)* (pp. 1-10). IEEE.

Mimecast. (2024). *Annual Data Exposure Report 2024*. Mimecast. https://www.mimecast.com/resources/white-papers/annual-data-exposure-report-2024/

Mohammed, M. A., Kadhem, S. M., & Maisa'a, A. A. (2021). Insider attacker detection using light gradient boosting machine. *Tech-Knowledge, 1*(1), 67-76.

Nabil, E., Sayed, S. A. F., & Hameed, H. A. (2020). An efficient binary clonal selection algorithm with optimum path forest for feature selection. *International Journal of Advanced Computer Science and Applications*, *11*(7).

Nicolaou, A., Shiaeles, S., & Savage, N. (2020). Mitigating insider threats using bio-inspired models. *Applied Sciences*, *10*(15), 5046.

Noever, D. (2019). Classifier suites for insider threat detection. *arXiv preprint arXiv:1901.10948*.

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. In *2014 IEEE security and privacy workshops*. IEEE. https://doi.org/10.1109/spw.2014.38

Padmavathi, G., Shanmugapriya, D., & Asha, S. (2022a). A Framework for Improving the Accuracy with Different Sampling Techniques for Detection of Malicious Insider Threat in Cloud. In *Proceedings of International Joint Conference on Advances in Computational Intelligence: IJCACI 2021* (pp. 485-494). Singapore: Springer Nature Singapore.

Padmavathi, G., Shanmugapriya, D., & Asha, S. (2022b). Detection of Malicious Insider in Cloud Environment based on behavior Analysis. In *Progressions made in Cyber-Security World* (pp. 1-9). CRC Press.

Pal, P., Chattopadhyay, P., & Swarnkar, M. (2023). Temporal feature aggregation with attention for insider threat detection from activity logs. *Expert Systems with Applications*, *224*, 119925.

Palmer, V. (2025). Systematic Literature Review on Insider Threat: Is the Australian Aviation Industry Complacent or Just Not Understanding Insider Threat?. *Journal of the Air Transport Research Society*, 100060.

Pantelidis, E., Bendiab, G., Shiaeles, S., & Kolokotronis, N. (2021, July). Insider threat detection using deep autoencoder and variational autoencoder neural networks. In *2021 IEEE International conference on cyber security and resilience (CSR)* (pp. 129-134). IEEE.

Peng, J., Choo, K. K. R., & Ashman, H. (2016). User profiling in intrusion detection: A review. *Journal of Network and Computer Applications*, *72*, 14-27.

Pengfei, J., Chunkai, Z., & Zhenyu, H. (2014, January). A new sampling approach for classification of imbalanced data sets with high density. In *2014 international conference on big data and smart computing (BIGCOMP)* (pp. 217-222). IEEE.

Pentel, A. (2017, July). Predicting age and gender by keystroke dynamics and mouse patterns. In *Adjunct Publication of the 25th Conference on User Modeling, Adaptation and Personalization* (pp. 381-385).

Prasad, P. S. S., Nayak, S. K., & Krishna, M. V. (2024). Enhanced Insider Threat Detection Through Machine Learning Approach With Imbalanced Data Resolution. *Journal of Theoretical and Applied Information Technology*, *102*(3).

Proofpoint, Inc. (2022, January 25). Global Cybersecurity Study: Insider Threats Cost Organizations $15.4 Million Annually, up 34 Percent from 2020. *GlobeNewswire News Room*. https://www.globenewswire.com/news-release/2022/01/25/2372208/35374/en/Global-Cybersecurity-Study-Insider-Threats-Cost-Organizations-15-4-Million-Annually-up-34-Percent-from-2020.html

PUTRA, S. R., & CHOWANDA, A. (2025). KEYSTROKE DYNAMICS ON MULTI-SESSION AND UNCONTROLLED SETTINGS USING CNN BI-LSTM. *Journal of Theoretical and Applied Information Technology*, *103*(2).

Rahman, M. H., Al Naeem, M. A., & Abubakar, A. (2022). Threats from unintentional insiders: An assessment of an organization's readiness using machine learning. *IEEE Access*, 10, 110294-110308.

Randive, K., Mohan, R., & Sivakrishna, A. M. (2023). An efficient pattern-based approach for insider threat classification using the image-based feature representation. *Journal of Information Security and Applications*, *73*, 103434.

Raskin, V., Taylor, J. M., & Hempelmann, C. F. (2010, September). Ontological semantic technology for detecting insider threat and social engineering. In *Proceedings of the 2010 New Security Paradigms Workshop* (pp. 115-128).

Raul, N., Shankarmani, R., & Joshi, P. (2020). Non-conventional factors for keystroke dynamics as a support factor for authenticating user. *Int. J. Innov. Technol. Exploring Eng.*, *9*(4), 474-479.

RM, B., & MK, J. K. (2023). Intrusion detection on AWS cloud through hybrid deep learning algorithm. *Electronics*, *12*(6), 1423.

Rust-Nguyen, N., Sharma, S., & Stamp, M. (2023). Darknet traffic classification and adversarial attacks using machine learning. *Computers & Security*, *127*, 103098.

S Zeid, S., A ElKamar, R., & I Hassan, S. (2022). Fixed-Text vs. Free-Text keystroke dynamics for user authentication. *Engineering Research Journal (Shoubra)*, *51*(1), 95-104.

Sahu, C., Banavar, M., & Schuckers, S. (2022). A novel non-linear transformation based multi user identification algorithm for fixed text keystroke behavioral dynamics. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, *5*(2), 277-287.

Saini, B. S., Singh, P., Nayyar, A., Kaur, N., Bhatia, K. S., El-Sappagh, S., & Hu, J. W. (2020). A three-step authentication model for mobile phone user using keystroke dynamics. *IEEE Access*, *8*, 125909-125922.

Salem, A., Sharieh, A., & Jabri, R. (2023). Online user authentication system using keystroke dynamics. *Journal of Computer Security*, *31*(3), 185-215.

Salem, M. B., Hershkop, S., & Stolfo, S. J. (2008). A survey of insider attack detection research. *Insider Attack and Cyber Security: Beyond the Hacker*, 69-90.

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. *Electronics*, *9*(9), 1460.

Sayegh, E. (2023). *Top cybersecurity predictions 2023*. Forbes. https://www.forbes.com/sites/emilsayegh/2022/12/15/top-cybersecurity-predictions-2023/?sh=36224e8c383f.

Sharma, A., Jureček, M., & Stamp, M. (2025). Keystroke dynamics for user identification. In *Machine Learning, Deep Learning and AI for Cybersecurity* (pp. 601-622). Springer, Cham.

Shekhawat, K., & Bhatt, D. P. (2022). A novel approach for user authentication using keystroke dynamics. *Journal of Discrete Mathematical Sciences and Cryptography*, *25*(7), 2015-2027.

Sheykhkanloo, N. M., & Hall, A. (2020). Insider threat detection using supervised machine learning algorithms on an extremely imbalanced dataset. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *10*(2), 1-26.

Shi, C., Liu, J., Liu, H., & Chen, Y. (2021). WiFi-enabled user authentication through deep learning in daily activities. *ACM Transactions on Internet of Things*, *2*(2), 1-25.

Singh, M., Mehtre, B. M., & Sangeetha, S. (2022). User behavior based insider threat detection using a multi fuzzy classifier. *Multimedia Tools and Applications*, *81*(16), 22953-22983.

Singh, M., Mehtre, B. M., Sangeetha, S., & Govindaraju, V. (2023). User behaviour based insider threat detection using a hybrid learning approach. *Journal of Ambient Intelligence and Humanized Computing*, *14*(4), 4573-4593.

Singh, S., Inamdar, A., Kore, A., & Pawar, A. (2020, July). Analysis of algorithms for user authentication using keystroke dynamics. In *2020 International Conference on Communication and Signal Processing (ICCSP)* (pp. 0337-0341). IEEE.

Sumitra, B., Pethuru, C. R., & Misbahuddin, M. (2014). A survey of cloud authentication attacks and solution approaches. *Int. J. Innov. Res. Comput. Commun. Eng*, *2*(10), 6245-6253.

Tao, X., Liu, J., Yu, Y., Zhang, H., & Huang, Y. (2025). An insider threat detection method based on improved Test-Time Training model. *High-Confidence Computing*, 100283.

Tewari, A., & Verma, P. (2022). An improved user identification based on keystroke-dynamics and transfer learning. *Webology*, *19*(1), 5369-5387.

Thapliyal, A., Verma, O. P., & Kumar, A. (2022). Behavioral biometric based personal authentication in feature phones. *International Journal of Electrical and Computer Engineering*, *12*(1), 802.

Trivedi, A. (2025). Research Paper on Cybersecurity and Insider Threat Detection: The Role of User Behavior Analytics (UBA) in Modern Defense Strategies. *International Journal for Research in Applied Science and Engineering Technology*, *13*(1), 455–466. https://doi.org/10.22214/ijraset.2025.66298

Van Ede, T., Aghakhani, H., Spahn, N., Bortolameotti, R., Cova, M., Continella, A., ... & Vigna, G. (2022, May). Deepcase: Semi-supervised contextual analysis of security events. In *2022 IEEE Symposium on Security and Privacy (SP)* (pp. 522-539). IEEE.

Verizon. (2023). *2023 Data Breach Investigations Report Public sector snapshot*. https://www.verizon.com/business/resources/Ta5a/reports/2023-dbir-public-sector-snapshot.pdf

Verizon. (2024). *2024 Data Breach Investigations Report*. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

Waiganjo, I. N., & Nandjenda, L. S. (2025). Unveiling Insider Threats: Examining Vulnerabilities in an Organizational Structure: A Case Study of NamPost. *Open Access Library Journal*, *12*(1), 1-10.

Wang, X., Fidge, C., Nourbakhsh, G., Foo, E., Jadidi, Z., & Li, C. (2022). Anomaly detection for insider attacks from untrusted intelligent electronic devices in substation automation systems. *IEEE Access*, *10*, 6629-6649.

Wang, X., Shi, Y., Zheng, K., Zhang, Y., Hong, W., & Cao, S. (2022). User authentication method based on keystroke dynamics and mouse dynamics with scene-irrelated features in hybrid scenes. *Sensors*, *22*(17), 6627.

Wang, X., Xu, J., Zeng, T., & Jing, L. (2021). Local distribution-based adaptive minority oversampling for imbalanced data classification. *Neurocomputing*, *422*, 200-213.

Wei, G., Guan, M., Ma, Y., Sun, R., Yuan, W., & Niu, Y. (2022, August). A high-performance malicious operation behavior detection model. In *International Conference on Cyber Security, Artificial Intelligence, and Digital Economy (CSAIDE 2022)* (Vol. 12330, pp. 381-386). SPIE.

Whitelaw, F., Riley, J., & Elmrabit, N. (2024). A review of the insider threat, a practitioner perspective within the UK financial services. *IEEE Access*, *12*, 34752-34768.

Yap, B. W., Rani, K. A., Rahman, H. A. A., Fong, S., Khairudin, Z., & Abdullah, N. N. (2014). An application of oversampling, undersampling, bagging and boosting in handling imbalanced datasets. In *Proceedings of the first international conference on advanced data and information engineering (DaEng-2013)* (pp. 13-22). Springer Singapore.

Yuan, F., Cao, Y., Shang, Y., Liu, Y., Tan, J., & Fang, B. (2018). Insider threat detection with deep neural network. In *Computational Science–ICCS 2018: 18th International Conference, Wuxi, China, June 11–13, 2018, Proceedings, Part I 18* (pp. 43-54). Springer International Publishing.

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

Yunanto, P. E., & Barmawi, A. M. (2022). Bimodal Keystroke Dynamics-Based Authentication for Mobile Application Using Anagram. *Jurnal Ilmu Komputer dan Informasi (Journal of Computer Science and Information)*, *81*, 91.

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*(1), 4148441.

Zhang, L., & Zhang, D. (2016). Evolutionary cost-sensitive extreme learning machine. *IEEE transactions on neural networks and learning systems*, *28*(12), 3045-3060.

Zhu, Y., Yan, Y., Zhang, Y., & Zhang, Y. (2020). EHSO: Evolutionary Hybrid Sampling in overlapping scenarios for imbalanced learning. *Neurocomputing*, *417*, 333-346.

Avinashilingam Institute for HomeScience and Higher Education for Women
(Deemed to be University Estd. u/s 3 of UGC Act 1956, Category 'A' by MHRD
Re-accredited with A++ Grade by NAAC. CGPA 3.65/4, Category I by UGC
Coimbatore - 641 043, Tamil Nadu, India

Appendix L2

(Item No 5 of Check List) Details of Research Publications

S.No	Article	Journal	Other Details Vol/No/Page No/ Year	Published in UGC-CARE / Scopus Indexed/ Web of Science
1	MALICIOUS INSIDER THREAT DETECTION USING VARIATION OF SAMPLING METHODS FOR ANOMALY DETECTION IN CLOUD ENVIRONMENT	COMPUTERS AND ELECTRICAL ENGINEERING	VOL: 105 NO: 108519 Pageno: 1 - 15 YEAR: 2023	WEB OF SCIENCE / Scopus/ UGC Care
2	UNDERSTANDING INSIDERS IN CLOUD ADOPTED ORGANISATIONS: A CURVEY ON TAXONOMIES, INCIDENT ANALYSIS, DEFENSIVE SOLUTIONS, CHALLENGES	FUTURE GENERATION COMPUTER SYSTEMS	VOL: 155, Pageno: 427 - 446, Year: 2024	WEB OF SCIENCE/Scopus/ UGC Care

*Proof of list of Journals from Internet to be attached along with copies of reprints.

Scholar : Aiswa. S

Supervisor : 25/11/24 16/12/24

Checked By:

HoD/Dean of Respective School

16/12/24

16/12/24 for Dean PSCS

The scholar Miss. Asha, S (20PHCSF005) has published her research articles in the following journals:

1. Computers and Electrical Engineering - indexed in Web of Science - Science citation Index Expanded,
2. Future Generation Computer Systems - indexed in Web of Science - Science citation Index Expanded.

This may be considered.

25.11.24.
Asst. Librarian

The above journal titles are indexed in Web of Science - Science citation Index expanded as of today 16.12.2024.

16.12.2024
Asst. Librarian.

Computers and Electrical Engineering 105 (2023) 108519

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Malicious insider threat detection using variation of sampling methods for anomaly detection in cloud environment

Asha S [a,*], Shanmugapriya D, Assistant Professor and Head [b], Padmavathi G, Professor and Dean [a]

[a] Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamilnadu 641043, India

[b] Department of Information Technology, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamilnadu 641043, India

ARTICLE INFO

Keywords:
Anomaly detection
Cloud security
Malicious insider
Machine learning
Performance evaluation
Sampling techniques

ABSTRACT

Machine learning (ML) techniques have currently been exploited for malicious insider threat (MIT) detection. The data variation between malicious and genuine user influences the ML model to misinterpret a malicious insider. Hence, the class imbalance problem (CIP) remains a challenging one. Regardless of the CIP in MIT detection, past research has a significant shortfall in deploying diverse sampling methods. i.e., undersampling and oversampling approach. This study proposed a novel double-layer architecture for MIT detection. The initial layer involves integration, transformation, and sampling system of data. In the sampling system, an efficient sampling approach is adopted to depreciate CIP among eight sampling techniques, depending on the performance of support vector machine (SVM) classifier. Nearmiss2 (NM-2) excels and is considered an optimal sampling technique. In the second layer, sampled data of NM-2 is employed in an anomalous MIT detection model using various anomaly detection techniques and evaluated with performance metrics. The main focus is to validate the solution for CIP in anomaly detection techniques with previous research. The proposed double-layer architecture with NM-2 and One-class SVM obtained recall and f-score of 100% and 78.72%. In contrast, it exhibits an accuracy of 82.46%, with a reasonable detection rate for MIT detection

1. Introduction

Cloud computing framework provides several metered services to businesses, organizations, or private sectors through the internet. This framework has intrinsic defense measures to confront active security threats in services such as infrastructure, platform, and software. However, it is challenging to regulate security threats in case of passive attacks. One of its kinds is a malicious insider threat (MIT) which is complicated to notice in an organization due to the silent nature of an attack. Once an insider threat is detected, the consequences are uncountable in the case of reputation and financial resources. The reason behind its severity is that a malicious insider is a trusted authorized user with legitimate access to sensitive credentials about an organization and its amenities. A malicious insider could rapidly embezzle confidential credentials without evidence by harnessing authority.

In recent years, more malicious insiders dissembled an organization and widespread in public due to its gigantic consequence.

* Corresponding author at: Ms Asha S, Avinashilingam Institute for Home Science and Higher Education for Women, India
E-mail addresses: 20phcsf005@avinuty.ac.in (A. S), shanmugapriya_it@avinuty.ac.in (S. D), padmavathi_cs@avinuty.ac.in (P. G).

https://doi.org/10.1016/j.compeleceng.2022.108519
Received 11 August 2022; Received in revised form 19 November 2022; Accepted 27 November 2022
Available online 2 December 2022

Including Marriott hotels and resorts, Elliott Greenleaf law firm, South Georgia Medical Center, Twitter, Ubiquiti Networks, Proofpoint, Saudi Aramco, Pfizer and UK Parliament [1], some organizations experienced MIT, leading to data leakage in 2021. In the 2022 cost of an insider threat global report conducted by Ponemon Institute, an insider threat maximized their occurrence and pecuniary loss over the past two years from 2020. Since then, the number of insider threat incident is doubled. Furthermore, the minimum number of cases reported for insider incidence remains one, whereas the uttermost is 46. The crime has been filed in the past 12 months, where malicious insiders were involved in 26% of cases.

It is analyzed that an incidence of insider threat multiplies intensely owing to an organization's size. The statistics reveal that 52% of respondents are worried about insider-driven data loss in a cloud environment [2]. The insider is able to compromise security checks by utilizing legitimate authority and trying to sneak confidential information by identifying loopholes. The main categories of insider threats are careless employees, malicious insiders and credential swindlers. The activities, including private information transmission to third parties, monitoring open ports and security flaws, obtaining or downloading sensitive information irrelevant to the role or function, and utilizing unauthorized USB flash drives ensuing unusual behavior on a regular working basis, are certain functionalities of malicious insiders.

Machine learning (ML) is persistently becoming more dominant in the domain of MIT. Nevertheless, preceding research has employed ML methods to categorize and recognize the behavior of malicious insiders. The challenging factor is preferring appropriate ML classification methods to acquire a supreme outcome in detecting MIT [3]. The appropriate model for eminent detection of MIT is evaluated using performance evaluation metrics, including precision, accuracy, f-score and recall. The performance of ML algorithms is susceptible to the concern of class imbalance (or class disparity issue). i.e., the phenomenon in which the occurrence of unusual behavior in an organization is much fewer than benign behavior. However, it would be tricky to classify the uneven class data owing to possible misclassification and misinterpretation. i.e., the ML classification model would consider a minority class of abnormal activities as an outlier and neglect it during classification. The inaccurate classification of minority class accompanies misinterpretation, followed by performance suppression in ML methods. The usage of data-level sampling methods could overcome misinterpretation. At present, various sampling methods are available that cover all aspects of a data-level sampling system. Therefore selecting an ideal sampling approach to address CIP is tricky. Most existing solutions utilize anomaly detection techniques. As a consequence, preferring the finest anomaly detection approach for exposing MIT using sampled data remains problematic. Anomaly detection techniques effectively observe abnormal activity against benign behavior relying on user actions. The eminent insider threat detection framework should combine sampling and anomaly detection techniques [4].

This paper proposes a two-layer system to address the challenges mentioned earlier. Eight prevailing variants of data-level sampling approaches in the first layer are explored under data pre-processing and sampling systems to attain symmetrically balanced data. Support Vector Machine is used to assess the findings of discrete sampling approaches using evaluation metrics to prevail the best adequate sampling method within a data sampling system. Depending on an output from the preceding layer, six anomaly detection techniques are employed in the subsequent layer using sampled data. These techniques are evaluated using the performance metrics noted previously to derive an ultimate anomaly detection technique to detect MIT. The contributions of this study are as follows:

- Novel intelligent double-layer architecture for adopting utmost sampling techniques and an anomaly detection algorithm for discovering insider threats has been developed.
- Exploring undersampling and oversampling approaches to unravel the class imbalance issue in Computer Emergency Response Team (CERT) synthetic datasets from Carnegie Mellon University.
- The proposed double-layer architecture has been analyzed, studied using the CERT dataset, and evaluated as per metrics such as precision, accuracy, f-score, and recall using False Positive (FP), False Negative (FN), True Negative (TN), and True Positive (TP).

The rest of the paper is structured as follows: The related works are discussed in Section 2. The background study is discussed in Section 3. The proposed two-layer architecture is described in Section 4. The performance analysis is elaborated in Section 5, and the final section concludes the paper with future scope.

2. Related works

At present, the solution for MIT identification through asymmetric class data is inadequate. Thereby, pinpointing a sufficient MIT detection approach is still complicated because imbalanced data uprises the class imbalance problem (CIP), and performance metrics such as recall, precision, accuracy and f-score are utilized for evaluating the models. The most promising model is preferred based on the performance of MIT detection.

Explored ML techniques for recognizing malicious insiders in [5] and evaluated based on accuracy, Area Under Curve (AUC) and recall using The Wolf of Sutd (TWOS) dataset. However, boosting techniques such as Adaboost [6], Extreme Gradient Boosting (XGBoost) [6], and Light Gradient Boosting Machine (lightGBM) [7] had successfully handled the CIP compared to other state-of-art methods. Another solution for better classification is to apply deep learning techniques. The performance of AutoEncoder (AE) and Variational AutoEncoder (VAE) for MIT detection is observed in [8]. In [9], three ML algorithms, namely Decision Tree (DT), Hidden Markov Model (HMM) and Self Organizing Maps (SOM), are evaluated to choose the best-performing algorithm based on mentioned performance criteria. However, VAE and SOM performed well and achieved a maximum detection rate with less False Positive Rate (FPR), thus outperforming other algorithms.

MIT detection using an imbalanced dataset is quite cumbersome, and hard to achieve better performance due to the CIP. It can be solved by applying a hybrid solution to the issue of class disparity in malicious insider anomaly detection. In [10], a framework was

Table 1
Review of significant research in classification and anomaly detection techniques for detection of MIT.

Study	Study scheme	Key findings	ML model scheme	Algorithms applied	Observations
[5]	Detection using imbalanced data	Evaluated six ML classifiers using the TWOS dataset to select the best-performing technique for MIT detection based on accuracy, recall and AUC.	Classification and regression	Adaboost, NB, LR, KNN, LR and SVM	Adaboost performed well and obtained accuracy, recall and AUC of 98.3%, 98% and 98.3%, outperforming other techniques for malicious emails using the TWOS dataset.
[6]	Detection in imbalanced data	Implemented user behavior analysis for MIT detection using XGBoost, and evaluated using accuracy, precision, recall and f-score.	Classification	RF, MLP and XGBoost	XGBoost performed better than other algorithms and obtained a 99.96% f-score using the CERT dataset for user behavior analysis.
[7]	Detection in imbalanced data	Introduced an intelligent framework for MIT detection using LightGBM and evaluated using f-score, AUC and accuracy.	Classification	LightGBM	Achieved an accuracy of 99.47% using imbalanced cert data and successfully obtained higher AUC and f-score for detecting the MIT event.
[8]	Detection in imbalanced data	Concentrated on highly imbalanced malicious insider data, AE and VAE were evaluated using performance metrics such as precision, recall, accuracy and f1-score.	Classification	AE and VAE	The performance of a VAE neural network provides the best result and obtained precision, recall, accuracy and f1-score of 92%, 96%, 96% and 94%, which is higher than AE and outperforms AE.
[9]	Detection in imbalanced dataset	Evaluated three ML algorithms to select the best algorithm to classify malicious behavior based on recall, FPR and accuracy.	Classification	SOM, HMM, and DT	SOM provides better results based on detection rate, false-positive rate, and accuracy in detecting insider threats using CERT data.
[10]	Detection using imbalanced data	A framework was proposed using supervised methods to detect the MIT and evaluated using balanced data via the Spread Subsample feature in the weka tool and imbalanced data in five classifiers based on precision, recall, f-score and time taken.	Classification	NB,LR, RF, SVM, and NNs	Classifiers with different parameters affected the performance metrics, but their impact was more substantial on an imbalanced dataset than on a balanced dataset.
[11]	Detection in balanced data	Applied oversampling technique, namely SMOTE, to handle CIP, and evaluated using three-time series classification methods based on precision, recall and f-sore.	Classification	IF, RF, and Deep AE	The performance of RF and Deep AE is comparable and achieves the best result for detecting MIT.
[12]	Detection in balanced dataset	Applied ADASYN for CIP and evaluated using DNN to detect the MIT.	Classification	Deep neural network (DNN)	The performance of DNN outperforms existing ML techniques using balanced data.
[13]	Detection in imbalanced data	Applied different ML techniques for successful MIT detection and evaluated using accuracy, kappa and time.	Classification	Bayesian model, linear regression, logistic regression, model tree, linear classifier, neural network, RF, SVM, Tree based model, Rule based model, Partial least squares, polynomial model.	Random forest obtained an accuracy of 98% and performed well than other classifiers.
[14]	Detection using imbalanced data	Proposed novel MIT detection framework using anomaly detection in an unsupervised ensemble approach using the CERT dataset	Anomaly detection	AE, IF, LODA and LOF	AE outperforms other algorithms based on voting metrics to detect MIT.
[15]	Detection in imbalanced data	A framework was proposed to model the zero-knowledge anomaly-based behavior for MIT detection.	Anomaly detection	LR, RF, and MLP	The performance of RF produces the best result for detecting MIT than other techniques.
[16]	Detection in imbalanced data	Designed anomaly detection using a graphical neural network, namely GCN, to detect abnormal malicious behavior and evaluate using other existing methods.	Anomaly detection	RF, SVM, LR, CNN and GCN	On the basis of accuracy, precision, and recall, GCN surpasses other algorithms.
[17]	Detection in imbalanced dataset	Proposed an ensemble of deep AE for anomaly detection, trained using normal and abnormal behavior, and evaluated based on accuracy.	Anomaly detection	Deep AE	Deep AE detects any malicious insider behavior with a minor FPR.

(*continued on next page*)

Table 1 (*continued*)

Study	Study scheme	Key findings	ML model scheme	Algorithms applied	Observations
[18]	Detection in imbalanced dataset	A multilayer framework was proposed using misuse insider threat detection and anomaly insider threat detection and evaluated using recall, precision, accuracy, f-score, AUC, FPR, FNR, TNR and computation time to detect known and unknown insider threats.	Anomaly detection	KNN and RF	The performance of a proposed hybrid model obtained accuracy and FPR of 99% and 29% and outperformed other state-of-art methods.
[19]	Detection in imbalanced data	Proposed a framework based on the behavior of malicious insiders that combines the k-means and PCA for anomaly detection using an imbalanced CERT r6.2 dataset.	Anomaly detection	K-means, PCA	The anomaly detection using the proposed combined framework has a detection rate of 89% and outperforms K-means and PCA based on cut-off values of 1%, 5%, 10%, 15%, 20%, 25%, and 30% cut-off.
[20]	Detection in imbalanced data	Introduced a combined intelligent framework that applies classification and graph methods to identify the MIT and evaluated using f-score, AUC, precision and recall.	Anomaly detection	IF, OCSVM, LOF, EE, ANN, Gnb, Bgc, RF and Gbc	The boosting techniques obtained f-score, recall, precision and AUC scores of 99% and outperformed other algorithms.
[21]	Detection in imbalanced data	Evaluated two unsupervised ensemble-based anomaly detection techniques using the temporal representation of data, namely concatenation, percentile and mean difference, to describe the user behavior changes for MIT detection.	Anomaly detection	AE and IF	The combination of percentile representation of data in AE outperforms IF and achieves a high detection rate with a low false-positive rate to detect MIT.
[22]	Detection in imbalanced dataset	A double-layer framework was proposed using LSTM and CNN and evaluated using AUC for MIT detection.	Anomaly detection	LSTM and CNN	LSTM and CNN-based anomaly detection performs well, obtained AUC = 0.9449, and detects maximum insider threat in CERT data.
[23]	Detection in balanced dataset	Proposed a new sampling technique, namely CGAN. Evaluated three oversampling methods using four anomaly detection techniques to effectively handle the CIP based on precision, recall, f-score, kappa and Mathews Correlation Coefficient (MCC) to perform multi-class classification.	Anomaly detection	RF, XGBoost, MLP and IDCNN	The anomaly detection using CGAN in four classifiers has obtained higher performance than ROS and SMOTE to perform multi-class classification.

introduced using a spread subsample feature to curb CIP in five supervised ML methods and evaluated based on the performance of five classifiers for MIT detection. It is observed that SVM and Naïve Bayes (NB) perform well compared to other ML techniques in this study. The performance can be further achieved by applying boosting algorithms. In [11], the CIP is suppressed using Synthetic Minority Over-sampling Technique (SMOTE), an oversampling technique to equalize data proportion, and verified the performance using three-time series classification methods, namely RF, Isolation Forest (IF) and deep AE using performance metrics such as precision, recall and f-score. Thus deep AE and RF worked better using balanced data. In [12], a framework is proposed comprising oversampling and ML techniques using the CERT dataset and evaluated using precision, recall, f-score and AUC. SMOTE is useful in equalizing class data and evaluated using six ML classifiers, namely Logistic Regression (LR), RF, NB, K-Nearest Neighbor (KNN), DT and Kernel- SVM (KSVM). In contrast, DT achieved an AUC of up to 99% and outperformed other techniques.

Apart from SMOTE, Adaptive Synthetic (ADASYN) is highly recommended with Deep Neural Network (DNN) [12] to deal with CIP in MIT detection. In [13], 88 ML algorithms are explored to select the best-performing technique concerning the evaluation metrics such as kappa, time and accuracy. In contrast, RF achieved accuracy equal to 98% and outperformed other techniques. Furthermore, it is complicated to detect new MIT using classification algorithms; therefore, anomaly detection techniques are explored.

The anomaly detection using unsupervised ensemble learning algorithms, namely AE, IF, Local Outlier Factor (LOF) and Light-weight On-line Detector of Anomalies (LODA), are implemented in [14], while AE achieved better results and outperformed other algorithms. Furthermore, zero-knowledge anomaly-based behavior [15] was analyzed using LR, RF and MLP. RF performed well and achieved the best result. The application of an anomaly detection model using a Graph Convolutional Network (GCN) was introduced in [16]. It evaluated the performance among other algorithms, namely RF, SVM and Convolutional Neural Network (CNN), using accuracy, precision and recall. In comparison, GCN outperforms other algorithms for malicious activity detection. Moreover, the deep AE was recommended by [17] for MIT detection to manage misclassification with a lower false-positive rate.

MIT has been the subject of several types of research in recent years. Indeed, merely countable hybrid solutions are presented. A hybrid combination of KNN and RF was proposed by [18] to spot familiar and unfamiliar MIT. In [19], the proposed hybrid model fuses Principal Component Analysis (PCA) and k-means in anomaly detection for recognizing abnormal behavior using an imbalanced CERT dataset and evaluated using a detection rate. It outperforms K-means and PCA and obtained 89% accuracy. However, the performance could have been more satisfactory. A combined framework was recommended in [20] using classification and graph methods for MIT detection. Nine classifiers were applied and evaluated based on f-score, AUC, precision and recall. However, boosting techniques obtained a maximum detection rate and outperformed other algorithms.

The hybrid approach made up of a temporal representation of data in anomaly detection techniques such as AE and IF was applied and evaluated in [21] for locating employee behavioral change in imbalanced data, thus obtaining the best performance while combining percentile representation with AE. In addition, the hybrid approach in deep learning for anomaly detection is beneficial and was recommended by [22], using CNN and Long-Short Term Memory (LSTM) for behavior modeling. As a result, it obtained an AUC of up to 94.49% using an imbalanced CERT dataset.

Apart from SMOTE and ADASYN, a novel sampling technique, namely Conditional Generative Adversarial Network (CGAN), was proposed in [23] and evaluated using four ML techniques, namely RF, XGBoost, MLP and Intelligent Deep Convolution Neural Network (IDCNN). In this study, results proved that the performance of CGAN compromised ROS and SMOTE.

Four pivotal restrictions have been witnessed in Table 1, which outlines contemporary analysis for MIT detection. They are (i) The function of CIP impacts existing classification techniques and induces misclassification, augmenting a false detection rate. Few existing methods complement bagging and boosting algorithms to detract a false detection rate. However, these methods contribute adversely to exploring alternative ML techniques. (ii) The sampling technique is endorsed to compress the CIP within classification techniques. Besides, attaining an uttermost performance equivalent to boosting algorithms is complicated. (iii) Perceiving new MIT is troublesome in a classification technique. Accordingly, anomaly detection techniques are implemented. (iv) Proposing a hybrid approach for detecting malicious insiders using anomaly detection with an elevated detection rate is yet oppressive. However, fulfilling a maximal performance in various classification and anomaly detection techniques with imbalanced data is still disputing.

Regardless of substantial efforts in discerning malicious insiders, the previous studies have neglected existing undersampling and oversampling approaches to depreciate the CIP and have failed to incorporate within anomaly detection techniques for recognizing MIT. Despite the popularity of anomaly detection techniques, no prior study has attempted to use them as a solution to detect MIT.

Hence, an effort has been made to resolve a research gap in managing CIP using sampling approaches in data pre-processing and MIT detection using anomaly detection techniques to perceive MIT in the cloud.

3. Background studies

MIT has become a well-known concern and is regarded as one of the most significant cybersecurity issues [24]. It defines that MIT needs specialized detection methodologies, systems, and tools, as well as a capacity to identify them efficiently and precisely. Much research on MIT detection and related fields has been conducted to counter this complicated issue. However, sampling techniques for CIP in MIT detection are still to be explored.

3.1. Sampling techniques

It is necessary to balance instances of genuine and malicious users using sampling techniques where an instance of a malicious user is comparatively less than a genuine user. Previous work shows that the CIP can be solved using data-level, algorithmic-level and ensemble learning [25]. The data level approach is a part of pre-processing techniques that seek to balance data using undersampling and oversampling approaches [25] by adjusting a data distribution pattern. In oversampling, the number of minority samples is generated until the size equals the number of majority samples. In undersampling, the numbers of majority samples are eliminated until the size of both a majority and a minority sample remains the same

3.1.1. Oversampling approaches

The procedure of oversampling is to reproduce an instance of MIT until a class size becomes proportional as an instance size of MIT expands unexpectedly and a model learning time advances [25]. Random Oversampling, SMOTE and ADASYN are oversampling approaches applied to suppress class variation. a) Random Oversampling (ROS)

In oversampling, ROS is considered one of the familiar techniques. However, it randomly procreates an instance of MIT by reciting a minority class instance. Consequently, it stimulates concern about overfitting. b) Synthetic Minority Oversampling Technique (SMOTE)

Artificial synthetic methods are recommended to overcome overfitting in [26]. Regular, Borderline using KNN and SVM [26] are considered different approaches for generating minority malicious insider instances. In Eqn. (1), a process of SMOTE is to encompass malicious insider instances, and x_{zi} interpolation in KNN generates unique synthetic data to induce proportional data.

$$x_{new} = x_i + \lambda(x_{zi} - x_i)_{zi} \tag{1}$$

c) Adaptive Synthetic (ADASYN)

An enhanced version of SMOTE is known as ADASYN, which alters an artificial instance of a minority class in terms of each class weight. Following a size of nearby class instances, it produces discrete MIT instances [25]. The ultimate focus of this technique is

minority MIT instances.

3.1.2. Undersampling approaches

The undersampling approach's primary constraint is removing a genuine user instance until the class is proportional. Learning time is reduced when an instance size of a genuine user is reduced [25]. This study focuses on five undersampling strategies for balancing data skewed by class. They are Random Undersampling, Nearmiss1 (NM-1), Nearmiss2 (NM-2), Tomek-Link and Edited Nearest Neighbor. a) Random Undersampling (RUS)

RUS is one of the most prevalent undersampling approaches. It randomly reduces genuine user instances until a size equals minority MIT instances [27]. Consequently, critical knowledge is lost in a significant genuine user instance. It results in misinterpretation during classification. b) Nearmiss

Nearmiss works by resampling a genuine user instance required to distinguish every class. Instances of a genuine user in NM-1 are chosen when N nearby MIT instances meet a minimal intermediate gap. Meanwhile, in NM-2, a respective instance of genuine users is chosen unless N outermost MIT instances fulfil the smallest average distance.

(c) Tomek-Link (T-L)

The primary goal of T-L [27] is to perform like a classifier to diminish a majority instance by eradicating an outlier, and an equation is formulated below. From an Eq. 2, it is observed that the connection occurs if two instances of different classes are close to each other, an interval amid two instances is denoted as d.

$$d(x,z) < d(x,y)\, or\, d(y,z) < d(x,y) \tag{2}$$

d) Edited Nearest Neighbor (ENN)

The idea behind the ENN is to remove occurrences that do not fulfil a neighbour in KNN. The varieties of undersampling and oversampling approaches and their operating requirements are detailed in Table 2.

Therefore, various undersampling and oversampling relevant techniques for revealing MIT are examined for anomaly detection. The performance of various sampling techniques is evaluated using performance metrics to select the best sampling method for anomaly detection.

3.2. Machine learning-based anomaly detection techniques

The anomaly detection techniques applied using ML methods in balanced data are discussed in this section to differentiate the malicious insider from the genuine user. They are One-Class Support Vector Machine, Robust Covariance, Isolation Forest, Local Outlier Factor, Lightweight on-line detection of Anomalies and K-Nearest Neighbor.

3.2.1. One-Class Support Vector Machine (OCSVM)

To squelch the challenge of classification model training adopting just one class of instances, an enhanced traditional SVM technique, namely OCSVM, is used for a key pattern generation from target class distribution, considered as a principal advantage of OCSVM. The OCSVM algorithm is outlined below. (a) From dataset X, identify training and test samples such as Xa and Xb. (b) Normalization is utilized to shorten training time and ensures model convergence. (c) To identify the optimum parameter combination (g, υ), always choose the function as an RBF kernel and apply a grid search for cross-validation. (d) Construct, build and train the OCSVM model for anomaly detection.

3.2.2. Isolation Forest (IF)

IF is a kind of ensemble technique that isolates abnormal data points to compute an isolation tree (iTree) for anomaly detection with maximum precision and computation rates. A major challenge is a less anomalous detection rate when data distribution becomes complex. The combination of more iTree is known as IF.

Let T be a single node in iTree. An internal node may consist of two daughter nodes (Tl, Tr) and one test. Assuming Q and P are

Table 2
Sampling techniques and their working criteria.

Sno	Sampling technique	Sampling type	Sampling mechanism	Working pattern
1	ROS	Oversampling	Prototype selection (controlled oversampling)	Random based
2.	SMOTE	Oversampling	Prototype selection (controlled oversampling)	KNN interpolation
3.	ADASYN	Oversampling	Prototype selection (controlled oversampling)	Adjacent class instance
4	RUS	Undersampling	Prototype selection (controlled undersampling)	Random based
5	NM-1	Undersampling	Prototype selection (controlled undersampling)	distance-based on minimum average (N adjacent MIT instances)
6	NM-2	Undersampling	Prototype selection (controlled undersampling)	distance-based on minimum average (N extreme MIT instances)
7	T-L	Undersampling	Prototype selection (cleaning undersampling)	Link based
8	ENN	Undersampling	Prototype selection (cleaning undersampling)	KNN based

attributes from dataset X to construct iTree and repeatedly segregate by its property $x_i(Q)$ unless either requirement embodies: (a) On the nodes, there seems to be single data; (b) The same constraints have to be followed by a node data; (c) Boundary for the tree height is attained. If and only if the value of P is more than $x_i(Q)$, the value of $x_i$is placed in the left subtree and vice versa. (b) For dataset X, the average tree path length, c(n), is calculated. (c) An anomalous score is calculated using Eq. 3 for the data point x.

$$s(x,n) = 2^{-\mathrm{E}\frac{(h(x))}{c(n)}} \tag{3}$$

Where, the chance of being recognized as an outlier is high when$\mathrm{E}(h(d)) \to 0,\ s \to 1$. However, the possibilities are slim when$\mathrm{E}(h(d)) \to n,\ s \to 0$.

3.2.3. Robust Covariance (RC)

The algorithm applying Mahalanobis distance in an unsupervised technique to detect an outlier is called Robust Covariance. The process is described below: (a) initially, identify a subset that has minimum determinant and h samples from dataset X. (b) Furthermore, construct an average value estimator of Xi data points. (c) The covariance measure of Xi is calculated using a proportional factor. (d) Consequently, calculate a Mahalanobis distance between a centre and the data point. (e) The data is considered an outlier if the confidence coefficient is 97.5%. Some advantages of RC are high robustness and high efficiency.

3.2.4. Local Outlier Factor (LOF)

LOF applies unsupervised density methods for easy local outlier identification. The working of LOF is depicted below with eqn.8: (a) k-distance measure of p is defined as Nk(p), between point p and point o is calculated. (b) The k-distance reachability is calculated by $|N_k(p)| \geq k, \quad reach - dist_k(p,0)$ (c) Calculate the local-reachability density ($\mathrm{lrd_k(p)}$), and the formula is defined in Eq. 4. (d) If the value of $\mathrm{LOF_k(p)}$ is more than 1, point p might be identified as an outlier.

$$LOF_k(p) = \sum_{o \in N_k(p)} \frac{(lrd_k(o))}{lrd_k(p)} / |N_k(p)| \tag{4}$$

Table 3
Specification for six machine learning based anomaly detection algorithms.

Algorithm	Parameter	Value
OCSVM	Kernel	RBF
	polynomial kernel function's Degree	3
	Gamma value	Auto
	Nu value	0.12
	Maximum iteration	-1
IF	Number of estimators	100
	Maximum number of samples	Auto
	Contamination	0.1
	Maximum features	1.0
	Bootstrap	False
	Number of jobs	None
	Random state	None
	Verbose	0
RC	Stored estimated precision	True
	Assume center point	False
	Support the fraction	None
	Contamination	0.5
	Instance of random state	None
LOF	No of neighbors	35
	Algorithm	Auto
	Size of leaf	30
	Metric	Minkowski
	Metric parameter	2
	Metric function arguments	None
	Contamination	0.1
	Number of jobs in parallel	None
LODA	Contamination	0.1
	No of histogram bins	10
	No of random cuts	100
KNN	No of neighbors	
	Weights	Uniform
	Algorithm	Auto
	Size of leaf	30
	Minkowski power parameter	2
	Metric	Minknowski
	Parameter for metric function	None
	No of parallel jobs	None

3.2.5. Lightweight on-line detection of Anomalies (LODA)

LODA is a type of ensemble approach [14] that creates a robust classifier acquired by combining the collection of weak anomaly detector classifiers with fewer error rates. The working of LODA is explained below with Eq. 5

$$w_i \in \mathscr{R}_{i=1}^{d^k} \tag{5}$$

(a) Where, k one-dimensional vector creates non-zero components $\sqrt{d}$ to compute probability density per data point. (b) Compute a histogram per k vectors. (c) The distance between a variation of original data distribution per histogram is used for outlier identification. (d) Repeat the process to update a histogram bin and vectors. (e) The logarithm of probabilities is utilized to compute an anomaly score for data points based on single projection vectors.

3.2.6. K-Nearest Neighbor (KNN)

The KNN is a non-parametric lazy learning classification approach using Euclidean distance measures and requires no training time. As a result, it is seen as a significant benefit of KNN.

The following exemplifies the KNN algorithm: (a) Using data points, the approximation distance is calculated from input vectors. (b) The KNN has been mapped into unlabeled data points. (c) The selection of a k-parameter for the KNN classifier is required. (d) Choose an ideal number of neighbors for categorization. (e) To detect an abnormality, create and train a KNN classifier. An outlier is a data point that ultimately fails the k-neighborhood.

The parameter specification for six ML-based anomaly detection techniques, as above mentioned earlier, is demonstrated in Table 3.

4. Proposed double layer architecture

The working principle of a proposed double-layer architecture is developed to alleviate the risk of class disparity for MIT detection utilizing sampling methods. Fig. 1 illustrates the overview of a proposed double-layer architecture. The two primary purposes of a

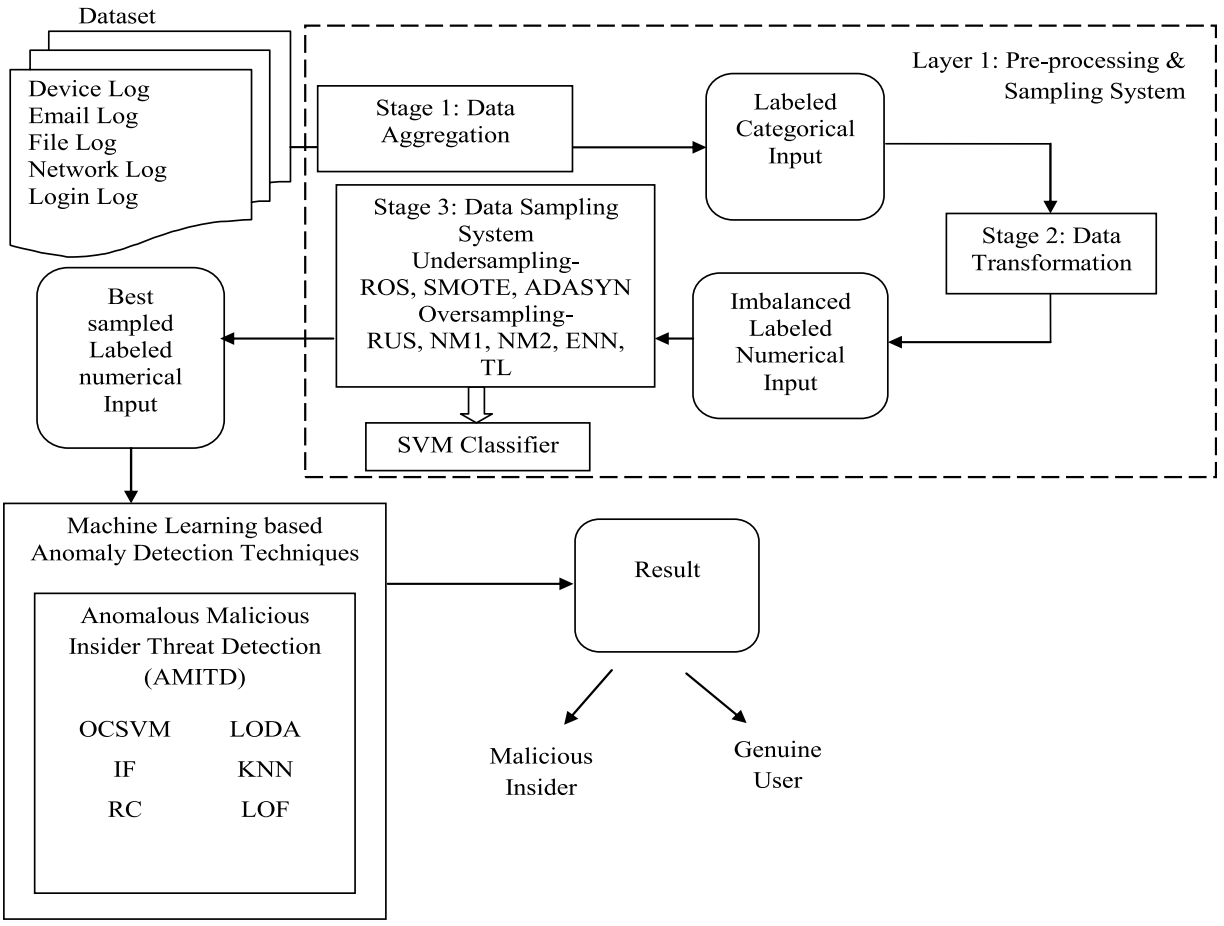

Fig. 1. Proposed double layer architecture.

proposed architecture are: (i) In the first layer, evaluating variants of sampling methods using an SVM classifier based on performance evaluation metrics and, thus, selecting a more effective sampling method. (ii) In the second layer, ML-based anomaly detection is applied to recognize malicious behavior using well-balanced data obtained from the first layer.

4.1. Layer 1: Pre-processing and sampling system

The sampling methods mentioned earlier have been explored to determine an efficient sampling approach. Therefore, the subsection discusses preprocessing techniques, such as data aggregation, data encoding or transformation, and selected sampling approaches used to unravel class dissimilarity issues in double-layer architecture.

4.1.1. Data Aggregation

In the baseline dataset described in Section 5.2, employee behaviors are kept in diverse records: logon, device, and HTTP. MIT detection in each table is time-consuming, so incorporating dissimilar tables into a single homogeneous table is necessary to perform anomaly detection. A simple feature concatenation technique can be applied to concatenate different tables [25,26].

4.1.2. Data transformation

Integrated data has six features: Insider Threat, Vector, Date, User, Pc and Activity. The variable types of these features are categorical and ordinal; date is the ordinal variable, and others are categorical. An ML method recognizes information solely in digital format. Consequently, the features in categorical format are converted into numerical ones using a categorical encoding technique [23]. The date can be transformed into several epochs. This study uses categorical encoding in data transformation to alter merged categorical information into numeric.

4.1.3. Data sampling system

Variants of the sampling approach have been employed in modeling data sampling systems using transformed data. Eight sampling approaches, among undersampling and oversampling, have been widely used to manage class disparity issues in classification techniques. The sampling methods include ROS, SMOTE, ADASYN, RUS, ENN, NM-1, NM-2 and T-L.

From the sampling techniques mentioned above, NM-2 generates well-balanced data by eliminating instances of a genuine user, which fails to achieve an intermediate interval between the N outermost instance of a malicious class. Accordingly, it performs well than other sampling techniques in the data sampling system.

However, no previous study has recognized the significance of any sampling method, raising a practical challenge in preferring a considerable optimal sampling approach.

4.1.4. Evaluation metrics

Numerous performance evaluation metrics have been used for evaluating the data sampling system. A confusion matrix with projected output is created for binary classification: False Negative (FN), False Positives (FP), True Negatives (TN), and True Positives (TP). Where TP is the number of precisely categorized MITs, TN is the amount of accurately classified genuine user behavior, and FP is the amount of mistakenly categorized genuine user behavior. FN is the size of incorrectly classified malicious behavior. Table 4 represents the performance metrics utilized for evaluating the performance of sampling methods.

4.1.5. SVM for Evaluation

The classification model, an SVM classifier, is modeled using sampled data from various sampling techniques mentioned earlier and evaluated for its performance. The precise classification results in diminishing class disparity issues. The balanced data needs to be assessed using an ML model that measures classification level. Since the present research satisfies binary classification, an SVM classifier is adopted to estimate the working of sampling methods in a data sampling system. Table 5 explains the simulation parameters of SVM. The sampled data is split into two main parts: train and test data to build a classification model. The SVM classifier was trained and tested using the train and test data.

The performance evaluation of an SVM classifier using sampled data depends upon evaluation metrics such as accuracy, precision,

Table 4
Performance metrics applied in this study.

Formula	Description
$\text{Precision} = \frac{TP}{(TP+FP)}$	A fraction of MIT samples is considered a malicious insider. As a result, it indicates a malicious insider.
$\text{Recall} = \frac{TP}{(TP+FN)}$	Recall, also called sensitivity, is a fraction of the threat samples strictly distinguished as a malicious insider.
$\text{F} - \text{score} = 2^{*}\left(\frac{(precision^{*}recall)}{(precision+recall)}\right)$	Also named F-measure is specified as a harmonic mean between recall and precision.
$\text{Accuracy} = \left(\frac{(TN+TP)}{(TN+TP+FN+FP)}\right)$	It is considered a general significance of a classifier and is defined as a fraction of correctly classified positive and negative entries.

Table 5
Simulation parameters of SVM.

Parameters	Values
Kernel	RBF
Gamma	0.001
Nu	0.02

recall and f-score. The SVM classifier is applied in sampling approach evaluation requirements, considered as attributes, and a data sampling approach that has been developed is assessed as an alternative in an SVM classifier. The optimal performance of an SVM classifier using a distinct sampling approach is considered an ideal sampling approach that successfully balances majority and minority instances with respect to the metrics, as mentioned earlier.

4.2. Layer two: Machine learning-based anomaly detection

Fig. 1 indicates that a superior outcome sampling approach is selected and used for anomalous MIT detection in the second layer, depending on outcomes from the previous layer. The balanced data utilized by various ML-based anomaly detection techniques, i.e., OCSVM, RC, LOC, LODA, KNN and IF, are trained to individualize malicious and genuine users in an AMITD model are examined as follows.

4.2.1. Anomalous MIT Detection (AMITD)

An anomalous MIT detection model effectively detects MIT using balanced data. This model applies six ML-based anomaly detection techniques using genuine and malicious behavior in balanced data to build an AMITD model. Subsequently, depending on the proportion of abnormal behavior of users, MIT is identified that differs from a genuine user. If the difference exceeds a certain level, that behavior is considered an outlier, and the user who performs such behavior is regarded as a malicious insider.

4.2.2. Evaluation metrics for decision making

The working of an AMITD model is analyzed using several performance evaluation metrics. Table 3 represents the performance metrics utilized for measuring the throughput of implemented anomaly detection techniques using ML algorithms.

5. Performance Discussion

This section examines the obtained results of double-layer architecture. Section 5.1 illustrates the execution environment. The information regarding a utilized dataset is described in Section 5.2. Section 5.3 elaborates on the experimental results of a proposed double-layer architecture. Section 5.4 compares the performance of anomaly detection techniques using the most acceptable sampling approach. Section 5.5 analyzes the performance of a proposed architecture with other existing state-of-the-art methods.

5.1. Execution Environment

When conducting experiments, the information regarding execution environments is specified. Used an anaconda platform for training and testing a proposed double-layer architecture that enforces sampling approach and ML-based anomaly detection techniques. It is free and open-source software and equips an environment for ML techniques using Jupyter Notebook. It has preconfigured basic libraries in Python 3.6, such as pandas and math, whereas others require preinstallation in an operating machine for later research.

5.2. Details of datasets

The benchmark data for this research was obtained from the CERT division of Carnegie Mellon University, which combines information from diverse sources to generate a synthetic MIT dataset [28]. However, this study applies the publicly available CERT v3.2 benchmark dataset with the condition that satisfies scenario1 and scenario2 in MIT [29]. It incorporates activity information that generated 135117169 log events from 1000 users with an interval of 516 days among two employees performed maliciously based on MIT scenarios.

Table 6
CERT MIT scenario.

Scenario	Description
1	Personal who works after wage-hour carries a portable device and upload sensitive details via unauthorized websites, namely wikileaks.org. Tries to resign from the organization.
2	Personal visits a career portal website to examine a business opponent's recruitment possibilities. The personal's anomalous activity increases the use of a portable device and resigns an organization in the future.

Logon activity and information related to browsing, file accessing, mailing, usage of removable drive, psychological measures, and lightweight directory access protocol (LDAP) are all included in the CERT dataset. As a result, this study was conducted utilizing data relating to the cyber activities of users in an attempt to determine MIT using existing synthetic data. This study considers a CERT dataset that satisfies scenario-1 and scenario-2 as baseline data. In this study, information in baseline data is combined and encoded using data aggregation and data encoding in the first layer.

5.2.1. MIT Scenarios

Table 6 depicts two satisfied situations for MIT in a CERT dataset. With respect to the scenarios mentioned above, a dataset has been categorized into genuine users and malicious insiders in a CERT dataset. The following procedure is carried out using a CERT dataset to characterize the behaviors of a genuine and malicious insider.

The well-sampled dataset is separated into a training-testing set for examining the proposed MIT detection model. The training set contains behaviors of genuine users and malicious insiders, satisfying two MIT scenarios in a CERT dataset. In contrast, the testing set confines the user activities of genuine and malicious insiders known in a training set. The working of an AMITD model using training and testing set from a balanced CERT dataset is mentioned below:

- The equalized CERT data was split into two subsets: a training set represents the first subset for model learning, and a testing set represents the second subset for MIT detection.
- A complete training subset is utilized for instructing an AMITD model to generate patterns for genuine user working behavior and abnormal malicious user behavior. Later, a testing set is utilized to test a model to identify the MIT.
- Later, a testing set is utilized to examine a model that could identify genuine and malicious behavior. If a particular behavior slightly seems abnormal and considered an MIT.

5.3. Experimental Results

The preliminary results from layer one and layer two in double-layer architecture are discussed in the following. Section 5.3.1 describes the selection of a sampling system by applying an SVM classifier based on performance metrics in Section 4.1.4. Section 5.3.2 defines the result of an anomalous MIT detection.

5.3.1. Results of first layer

The experimental result of data preprocessing and sampling systems in the first layer from the proposed double-layer architecture that includes data integration, data transformation and data sampling system is explained in the following subsections.

(i) Results of data integration

Table 7 shows the result of a data integration method using a simple feature concatenation technique for three tables mentioned in Section 4.1.1. The integrated table of baseline data corresponds to selected scenarios in a daily log such as http.csv, logon.csv and device.csv. In integrated data, the standard features of the three tables are date, user, pc, and activity. In contrast, the feature named 'vector' denotes the origin of data, and 'InsiderThreat' denotes activity either in the form of malicious or genuine.

(ii) Results of data transformation

The values of the data were gathered from integrated data. However, categorical features, namely 'InsiderThreat', 'vector', 'user', 'pc' and 'activity', are encoded into numerical data. ML models only consider numerics as input. For instance, in this study, 'date' is a timestamp value and should be converted into numerics. The values of the vector feature represent the origin of user behavior, such as logging status, device connectivity behavior and internet browsing behavior. Considering five distinct behaviors of a user in features mentioned earlier, they were encoded as numerics [30], i.e., log-in (0), log-out (1), connect (2), disconnect (3), and HTTP (4). Table 8 demonstrates an encoded value of a categorical variable during pre-data and post-data transformation.

(iii) Performance evaluation of SVM classifier

Based on encoded preprocessed data, the different sampling approaches using an SVM classifier in a data sampling system are illustrated in Table 9. The performance evaluation has been accomplished concerning four evaluation metrics in an SVM classifier.

The table shows performance evaluation based on four metrics using an SVM classifier. The maximum detection rate is determined by precision, whereas a recall achieves a precise detection rate. The overall performance of an SVM classifier is determined by accuracy. The f-score is used to compute the harmonic mean between recall and precision. The highest f-score is considered the most crucial factor based on performance. The minor variance between precision and recall is notable, whereas a higher value in accuracy

Table 7
Performance result of a data integration method using a simple feature concatenation technique.

Feature name	Description
Insider threat	The category of activity either malicious activity or not
Vector	The source of information
Date	Date for every single event
User	An identification number that denotes the user performs a specific action
Pc	An identification number that denotes the computer where the action is performed
Activity	It denotes the particular action from every user

Table 8
Result of data transformation technique using categorical encoding.

Feature name	Pre-data Transformation	Post-data Transformation
Insider threat	1	1
Vector	Logon	0
Date	07-01-2010 02:23:00	1280707200
User	CCH0959	4
Pc	PC-0588	128
Activity	http://linkedin.com/jobs/displayhome.html	750

Table 9
Outcome of distinct sampling approaches.

Techniques Applied	Accuracy	F-score	Precision	Recall
Oversampling Techniques				
ADASYN	0.680375	0.80±0.03	0.99±0.02	0.67±0.77
ROS	0.680375	0.80±0.03	0.99±0.02	0.67±0.77
SMOTE	0.680375	0.80± 0.03	0.99±0.02	0.67±0.77
Undersampling Techniques				
ENN	0.680375	0.80± 0.03	0.99±0.02	0.67±0.77
NM-1	0.319625	0.48±0.00	0.97±0.00	0.32±0.22
NM-2	**0.84325**	**0.91±0.02**	**0.99±0.01**	**0.84±0.28**
RUS	0.716625	0.80±0.03	0.99±0.02	0.71±0.74
T-L	0.680375	0.80± 0.03	0.99±0.02	0.67±0.77

and precision is regarded as the least important.

(iv) Results of SVM classifier in data sampling system

The performance result of various sampling approaches in a data sampling system based on an SVM classifier is discussed in this subsection. An SVM classifier is evaluated using previously specified four evaluation metrics. It is noteworthy to consider accuracy, recall, precision and f-score.

Table 9 demonstrates the impacts of an SVM classifier, implying distinct sampling approaches. It is noted that the outcome remains identical for ROS, SMOTE and ADASYN. In addition, correctly classified genuine behavior is more diminutive. Therefore, it is complex to confront issues of class disparity with oversampling methods.

In contrast, the value of the f-score using the NM-1 undersampler is nearly insignificant, and the detection rate of malicious activity is insufficient. ENN and T-L outcomes are closer to similar and could be tolerable. However, NM-2 enhanced the creation of synthetic MIT instances and outperformed ROS. Consequently, it obtained maximum effect in four performance metrics as mentioned earlier than oversampler.

Therefore, the best sampling approach is selected based on the above analysis. The result is compared with the outcomes of an SVM classifier utilizing disparate data listed in Table 10.

Table 10 noticed that malicious activity is never witnessed by an SVM classifier using disparate data. In contrast, considering balanced data in an SVM classifier, it accurately signified non-malicious actions and obtained a higher recall value than disparate data. Meanwhile, balanced data acquired reasonable precision and f-score and exceeded disparate data, along with sufficient accuracy, to discover malicious actions. Hence, NM-2 is considered the best-performing sampling approach in a data sampling system using an SVM classifier based on the metrics mentioned above.

5.3.2. Results of second layer

The best sampling approach is selected, relying on its performance from the previous layer to obtain well-balanced data for modeling a consecutive layer of double-layer architecture for MIT detection. Corresponding to the outcome from Table 9, it is noteworthy that the NM-2 sampling approach outperforms other sampling approaches to crack CIP. Therefore, the architecture of the second layer contains a primary module: (i) An AMITD applies various ML-based anomaly detection techniques. An AMITD module uses a balanced sample using NM-2 from a data sampling system to build six anomaly detection methods that differentiate malicious from the genuine user corresponding to user behavior. The leading anomaly detection technique is selected based on performance metrics mentioned in Table 3 for insider threat detection.

(i) AMITD

Table 10
Pre and post undersampling technique.

Training set	Pre Sampling	Post Sampling
Majority class Non-Malicious activity instance	(0, 39732)	(0, 268)
Minority class Malicious activity instance	(1, 268)	(1, 268)

Initially, the working process of a suggested AMITD model is examined using sampled data, in which six anomaly detection techniques are trained using activities of both known MIT and genuine users. It implies that various anomaly detection techniques were trained and learned to generate a pattern based on the behavioral scenarios of a malicious insider. The results of a proposed AMITD model in a confusion matrix are given in Fig. 2.

Fig. 2 demonstrates the confusion matrix of six anomaly detection techniques for discovering MIT. The highest values in metrics, namely, true positive and true negative, indicate a fair outcome, compared with their lesser values denoting the poorest outcome. The declining values in negative standards, i.e., false positive and false negative, suggest the most promising outcome, but their elevated value demonstrates an inadequate outcome.

The performance of anomaly detection methods can be cross-verified using evaluation metrics, namely accuracy, precision, recall and f-score, and the result is depicted in Table 10. These metrics are considered positive evaluation criteria; the highest value denotes the most exemplary performance. In contrast, the declining value denotes downgrade performance. From the above noteworthy analysis, it is perceived that a proposed model delivers a desirable result since it has been trained using six anomaly detection algorithms and understood a pattern of atypical etiquette in accordance with the given scenarios of MIT.

5.4. Performance comparison

Fig. 2 shows that LODA and KNN provide similar outcomes and fail to detect malicious activity. i.e., a value of TN is 0. Hence, they are ignored. The false-negative for LOF and IF are 232 and 217. i.e., they consider numerous genuine activities as malicious and excluded as unsatisfying. RC highly misinterpreted both genuine and malicious activities and obtained a false positive and false negative rate of 119; consequently, it is cornered. The value of TN for OCSVM is 268, i.e., it predicts all malicious activities without misinterpretation. The comparative analysis shows that OCSVM outperforms other anomaly detection techniques in determining unusual actions in an organization.

Table 11 shows the values of evaluation metrics such as accuracy, recall, precision and f-score to measure the performance of six detection models in AMITD. It reveals that OCSVM obtained an accuracy of 82.46%, which is higher in contrast to other techniques in the AMITD model. Furthermore, correctly detected instances are higher in OCSVM and achieved 100% compared to 30%, 55%, 51%, 49.81% and 49.81% obtained by IF, RC, LOF, LODA and KNN. But, the detection rate or precision rate of OCSVM is 64.9%, which is lesser than 98.88%, 55.59%, 93.28%, 100% and 100% received by IF, RC, LOF, LODA and KNN. Therefore, it correctly predicted an entire detected instance without misinterpretation. Thus, it achieves a 78.72% f-score which is higher and outperformed other anomaly detection models in AMITD.

It is confirmed that OCSVM surpasses other anomaly detection techniques using sampled data from the first layer. Based on the accuracy, the performance of OCSVM is 25% higher than other anomaly detection models. It is observed that the f-score is 10% higher than other anomaly detection models, achieved 100% recall within a less detection rate, and surpassed other models

However, the above analysis prefers a comprehensive outcome of the OCSVM-based anomaly detection model, which is excellent to others. As a result, an AMITD model has been used to witness the behavior of MIT.

5.5. Comparisons with other existing state-of-the-art methods

The following section compares the outcome of a proposed novel AMITD model with alternate solutions from current state-of-the-art techniques. These outcomes were illustrated on the subject of the four evaluation metrics mentioned above and utilized to evaluate the AMITD model. Subsequently, an effect of a proposed AMITD model is compared with others comprised of deep learning, boosting techniques, and hybrid solutions for detecting malicious behavior, as portrayed in Table 12.

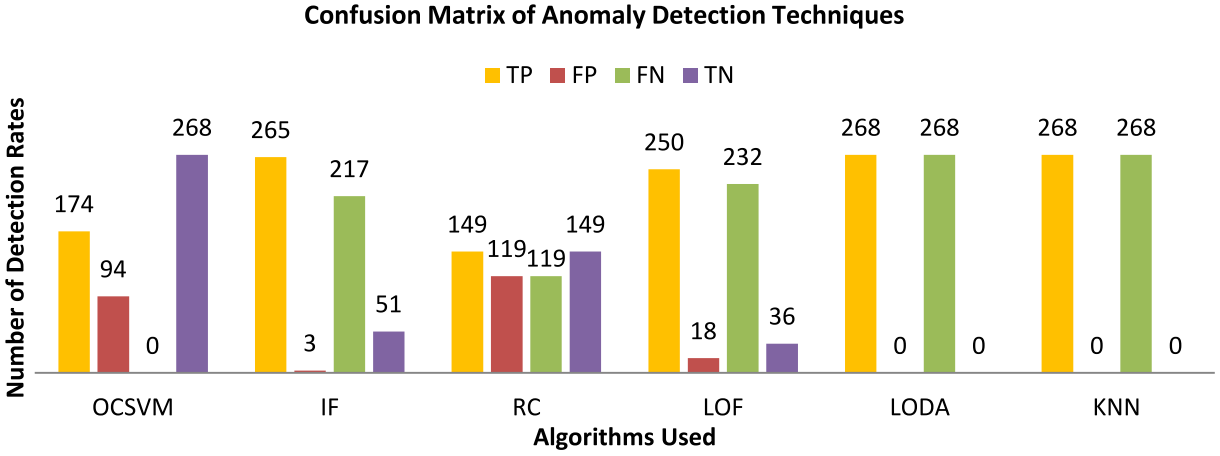

Fig. 2. The outcome of anomaly detection techniques in AMITD model.

Table 11
Performance of ML-based anomaly detection framework.

ML algorithms	Accuracy	Precision	Recall	F-score
OCSVM	**0.8246**	**0.6492**	**1**	**0.7872**
IF	0.5895	0.9888	0.3091	0.6112
RC	0.5559	0.5559	0.5559	0.5558
LOF	0.5335	0.9328	0.5186	0.6665
LODA	0.5	1	0.4981	0.6649
KNN	0.5	1	0.4981	0.6649

Table 12
Comparison of AMITD with other state-of-art methods.

Study	Method	Dataset	Results			
			Precision	Recall	F-score	Accuracy
[5]	Adaboost	TWOS	-	98%	-	98.3%
[7]	LightGBM	CERT	-	-	70.42%	98.03%
[9]	SOM	CERT	71.77%	-	-	88.38%
[11]	Random Forest	CERT	65.6%	80.71%	70.61%	-
[13]	Random Forest	CERT	-	-	-	98%
[15]	Random Forest	CERT	96.52%	-	75.42%	-
[18]	RF	CERT	51%	50%	49%	90%
[19]	Kmeans+PCA	CERT	89%	-	-	-
[23]	CGAN	CERT	79.12%	76.07%	74.85%	-
Proposed method	**OCSVM**	**CERT**	**64.92%**	**100%**	**78.72%**	**82.46%**

Table 12 adheres that a proposed method achieved 82.46% accuracy, which is lower than other methods. However, it gained 100% recall with a 78.72% f-score which is superior, and it successfully confronted the CIP and even excelled boosting technique. Accordingly, the contrast between an AMITD model and other present works reveals that a proposed novel method went beyond others with the utmost performance and detected an MIT precisely.

6. Conclusion and Future scope

In this study, an innovative double-layer architecture has been enforced to outdistance the restrictions of predominating MIT detection methods. The proposed architecture is assessed using CERT v3.2 dataset. A CERT dataset experiences primary preprocessing, i.e., data integration, transformation and sampling system during the initial layer of proposed architecture. A combined concealed data from the first two preprocessing techniques in the initial layer is sensible to classification using an ML model owing to the imbalanced number of instances between malicious and genuine users, and the CIP arises. But the sampling system in a proposed initial layer processes the CIP for MIT detection.

Furthermore, in a sampling system, the uniform data generated from various undersampling and oversampling techniques, i.e., NM-1, NM-2, T-L, RUS, ENN, ROS, SMOTE, and ADASYN, are exploited to model an SVM classifier. Subsequently, to prefer the finest sampling method, determine its performance using performance metrics such as precision, recall, f-score and accuracy. A surpass performance of NM-2 achieves the CIP and is utilized to perform ML-based anomaly detection techniques in an AMITD model from the second layer. In an AMITD model, six classifiers such as OCSVM, IF, RC, LOF, LODA and KNN, are modeled employing balanced data to individualize malicious insiders from genuine users. The performance of an AMITD model was valuated using precision, recall, f-score and accuracy. An OCSVM classifier accomplished the most promising outcome concerning the performance metrics, i.e., 100% recall, 79% f-score and 82% accuracy are considered in this work and other existing methods.

Ultimately, the composite framework for MIT revelation using a hybrid algorithm will probably be reconnoitred to maximize a proposed framework's detection rate or precision value.

CRediT authorship contribution statement

Asha S: Conceptualization, Methodology, Software, Validation, Formal analysis, Data curation, Writing – original draft, Visualization. **Shanmugapriya D:** Formal analysis, Investigation, Resources, Writing – review & editing, Supervision, Project administration, Funding acquisition. **Padmavathi G:** Formal analysis, Investigation, Resources, Writing – review & editing, Supervision, Project administration, Funding acquisition.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

I will share the DOI of public Insider Threat Dataset: 10.1184/R1/12841247.v1

Acknowledgments

The authors acknowledged Centre for Cyber Intelligence under DST - CURIE - AI - Phase II Project at Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamilnadu, India for providing infrastructural facilities.

References

[1] Ekransystem. 5 real-life data breaches caused by insider threats, https://www.ekransystem.com/en/blog/real-life-examples-insider-threat-caused-breaches. accessed 13 Apr 2022.
[2] Proofpoint. 2022 Cost of Insider Threat Global Report, https://static.poder360.com.br/2022/01/pfpt-us-tr-the-cost-of-insider-threats-ponemon-report.pdf. accessed 13 Apr 2022.
[3] Gheyas IA, Abdallah AE. Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. Big Data Anal 2016;1(1):1–29.
[4] Al-Mhiqani MN, Ahmad R, Zainal-Abidin Z, Yassin W, Hassan A, Abdulkareem KH, et al. A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations. Appl Sci 2020;10(15):5208.
[5] Janjua F, Masood A, Abbas H, Rashid I. Handling insider threat through supervised machine learning techniques. Procedia Comput Sci 2020;177:64–71.
[6] Jiang W, Tian Y, Liu W, Liu W. An insider threat detection method based on user behavior analysis. In International Conference on Intelligent Information Processing, Springer; 2018, p. 421-429.
[7] Mohammed MA, Kadhem SM, Maisa'a AA. Insider Attacker Detection Using Light Gradient Boosting Machine. Tech-Knowledge 2021;1(1):67–76.
[8] Pantelidis E, Bendiab G, Shiaeles S, Kolokotronis N. Insider threat detection using deep autoencoder and variational autoencoder neural networks. In 2021 IEEE International Conference on Cyber Security and Resilience (CSR), IEEE; 2021, p. 129-134.
[9] Le DC, Zincir-Heywood AN. Evaluating insider threat detection workflow using supervised and unsupervised learning. 2018 IEEE Security and Privacy Workshops (SPW). IEEE; 2018. p. 270–5.
[10] Sheykhkanloo NM, Hall A. Insider threat detection using supervised machine learning algorithms on an extremely imbalanced dataset. Int J Cyber Warfare Terrorism (IJCWT) 2020;10(2):1–26.
[11] Chattopadhyay P, Wang L, Tan YP. Scenario-based insider threat detection from cyber activities. IEEE Trans Comput Soc Syst 2018;5(3):660–75.
[12] Al-Mhiqani MN, Ahmed R, Abidin ZZ. Isnin S. An integrated imbalanced learning and deep neural network model for insider threat detection. Int J Adv Comput Sci Appl 2021;12(1).
[13] Noever D. Classifier suites for insider threat detection. ArXiv 2019;1901(10948).
[14] Le DC, Zincir-Heywood N. Anomaly detection for insider threats using unsupervised ensembles. IEEE Trans Netw Serv Manage 2021;18(2):1152–64.
[15] Ferreira P, Le DC, Zincir-Heywood N. Exploring feature normalization and temporal information for machine learning based insider threat detection. In 2019 15th International Conference on Network and Service Management (CNSM), IEEE; 2019, p. 1-7.
[16] Jiang J, Chen J, Gu T, Choo K-KR, Liu C, Yu M, Huang W, Mohapatra P. Anomaly detection with graph convolutional networks for insider threat and fraud detection. In MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM), IEEE; 2019, p. 109-114.
[17] Liu L, De Vel O, Chen C, Zhang J, Xiang Y. Anomaly-based insider threat detection using deep autoencoders. In 2018 IEEE International Conference on Data Mining Workshops (ICDMW), IEEE; 2018, p. 39-48.
[18] Al-Mhiqani MN, Ahmad R, Abidin ZZ, Abdulkareem KH, Mohammed MA, Gupta D, Shankar K. A new intelligent multilayer framework for insider threat detection. Comput Electr Eng 2022;97:107597.
[19] Garba N, Rakshit S, Mang CD, Vajjhala NR. An email content-based insider threat detection model using anomaly detection algorithms. In Proceedings of the International Conference on Innovative Computing & Communication, 2021, p. 1-5.
[20] Diop A, Emad N, Winter T, Hilia M. Design of an ensemble learning behavior anomaly detection framework. Int J Comput Inf Eng 2019;13(10):547–55.
[21] Le DC, Zincir-Heywood N. Exploring adversarial properties of insider threat detection. In 2020 IEEE Conference on Communications and Network Security (CNS), IEEE; 2020, p. 1-9.
[22] Yuan F, Cao Y, Shang Y, Liu Y, Tan J, Fang B. Insider threat detection with deep neural network. In International Conference on Computational Science, Springer; 2018, p. 43-54.
[23] Al-Shehari T, Alsowail RA. An insider data leakage detection using one-hot encoding, synthetic minority oversampling and machine learning techniques. Entropy 2021;23(10):1258.
[24] Padmavathi G, Shanmugapriya D, Asha S. A Framework to Detect the Malicious Insider Threat in Cloud Environment using Supervised Learning Methods. In 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), IEEE; 2022, p. 354-358.
[25] Padmavathi G, Shanmugapriya D, Asha S. A Framework for Improving the Accuracy with Different Sampling Techniques for Detection of Malicious Insider Threat in Cloud. In Proceedings of International Joint Conference on Advances in Computational Intelligence, Springer; 2022, p. 485-494.
[26] Zhu Y, Yan Y, Zhang Y, Zhang Y. EHSO: Evolutionary Hybrid Sampling in overlapping scenarios for imbalanced learning. Neurocomputing 2020;417:333–46.
[27] Elhassan T, Aljurf M. Classification of imbalance data using tomek link (t-link) combined with random under-sampling (rus) as a data reduction method. Global J Technol Optim S 2016;1.
[28] Lindauer B, Insider Threat Test Dataset. Carnegie Mellon University, v3; https://resources.sei.cmu.edu/library/asset-view.cfm.assetid=508099. </Dataset>.
[29] Nicolaou A, Shiaeles S, Savage N. Mitigating insider threats using bio-inspired models. Appl Sci 2020;10(15):5046.
[30] Hasanin T, Khoshgoftaar T. The effects of random undersampling with simulated class imbalance for big data. In 2018 IEEE international conference on information reuse and integration (IRI), IEEE; 2018, p. 70-79.

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Highlights

Understanding insiders in cloud adopted organizations: A survey on taxonomies, incident analysis, defensive solutions, challenges

Future Generation Computer Systems xxx (xxxx) xxx

Asha S.*, Shanmugapriya D.

- The comprehensive survey is well-versed for researchers in insider threat field.
- The survey anticipates four amalgamated taxonomies for classification are as follows:
- Insider threat incident; Custom defensive solution for detection-mitigation strategy;
- Collective information of publicly accessible benchmark datasets;
- Identify existing challenges in detection and mitigation to subside research directions;

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Review article

Understanding insiders in cloud adopted organizations: A survey on taxonomies, incident analysis, defensive solutions, challenges

Asha S. [a,*], Shanmugapriya D. [b]

[a] Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu 641043, India
[b] Department of Information Technology, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu 641043, India

ARTICLE INFO

Keywords:
Insider threat
Malicious insider threat
Masqueraders
Traitors
Unintentional insider threat

ABSTRACT

In cybersecurity, one of the most significant challenges is an insider threat, in which existing researchers must provide an extensive solution aiming at an enhanced security network. This study proposes a comprehensive taxonomy as well as a state-of-the-art research categorization according to the contribution of insider threat incidents and the defensive mechanism utilized against such insiders. The major objective of a proposed categorization is to provide structural information in the field of insider threat based on past research theories for analyzing literature review. The proposed categorization is classified into four groups: (i) dataset analysis, (ii) incident analysis, (iii) defensive solution, and (iv) encountered challenges. However, the respective taxonomies and annotations are included for complete insight into insiders. i.e., existing studies on systematic taxonomy based on incidents of insider threats are presented. The major contribution of this study in the area of insider threat is to deliver the following knowledge to upcoming domain specific researchers: (i) taxonomy in an innovative systematic approach concerning the categories of incidents and determine the possible defensive mechanism against insiders. (ii) a study on available benchmark datasets used by existing research for evaluating the defensive mechanisms. (iii) a brief description of past solutions and frameworks to model insider behavior with the aim of studying existing defensive mechanisms, and (iv) a short discussion of challenges encountered by defensive solutions based on existing research in the area of insider threat.

1. Introduction

In the era of information technology, the organization seeks flexible business solutions by means of platforms, software, and infrastructure, which can be accompanied by cloud computing as an integral framework that uses the internet as a medium to incorporate confidentiality, integrity, and availability of on-demand cloud resources. The organization recommends deploying cloud services in private and hybrid clouds to enhance security and privacy compared to a public cloud. Since cloud security is still an emerging challenge due to adopting its evolution, business information, including Intellectual Property Rights (IPR), and Personal Identification Information (PII) of stakeholders and customers stored in cloud storage remains at risk. However, threats in cloud security are categorized into two broad areas based on the nature of the ambush in an organization. i.e., Active attack and Passive attack. An active attack is a cyberattack involving an unauthorized individual attempting disruption in cloud-based systems and compromise them for confidential data and services. Unlike passive attacks, which involve illegitimate surveillance and eavesdropping on sensitive information in a perpetual manner carried by impertinent for self-curiosity, active attacks are more intrusive and aims at boundless manipulation, extinguishing, or exploiting the intended cloud resources.

Some of the common types of active attacks in a cloud-adopted organization contain misconfiguration and insufficient change control, hijacking of cloud accounts, weak control plane, lack of visibility in cloud usage, exploitation and despicable use of cloud services, cyber-attacks, denial of service attacks. Meanwhile, passive attacks such as malicious insider, deficiency in cloud security policy and architecture, insufficient management in terms of identity, credential, access and key, insecure interfaces and APIs, unauthorized access, and external data sharing are hard to recognize compared to active attacks. Due to the surreptitious nature and lack of active interruption to cloud-based data, most security measures in intrinsic cloud security target to recognize active attacks and leaving passive attacks behind them.

* Corresponding author.
E-mail address: 20phcsf005@avinuty.ac.in (Asha S.).

https://doi.org/10.1016/j.future.2024.04.033
Received 14 December 2023; Received in revised form 8 March 2024; Accepted 16 April 2024

However, passive attacks like insider threats are a significant concern for data security in a cloud-adopted organization.

Insider threat is an unauthorized individual who has legitimate access privileges to cloud-based systems containing sensitive information using valid credentials for personal curiosity. The chances of recognizing insider threats are less because of their trusted privileges, which results in massive information disclosure to unauthorized entities. In addition, it threatens cloud security and is presumably strenuous to detect. Thus, it inflicts immense damage on enterprises' reputations, financial assets, and intellectual property. The investigation reported by Forbes [1]: "Insiders often felt optimistic about being accompanied by an influential extortion hacker group named Lapsus to perform corporate malice, espionage, social engineering, and prognosticating may increase corporate targets in 2023". Another survey investigating top costly data breaches [2] highlights insiders' impact in some organizations in 2022, such as Revolut financial technology, Zoetop e-commerce, Nelnet Servicing, Twitter, Uber, Rockstar, Medibank, WhatsApp, and Optus telecommunications, which experienced massive impactful data breaches. According to a survey [3], the primary cause of data breaches is intentional monetary gain (49%), targeted outsiders (18%), impulsive data breaches (1%), and others (or unclassified). However, major vulnerable factors for stimulating insider-led data breaches include exploiting cloud vulnerability, abusive cloud service providers, sensitive information theft, and hosting malware in cloud services.

According to a data breach investigation report in 2022 [4], from 82% of individual-related breaches, outsider-related threats are 80% higher than insider threats. However, the probability of records being compromised by insiders is 76%, where 96% are for personal gain. Although the major consequence of such cases is a financial loss for the organization, it is also considered a law-breaking incident. Because, it questions business loyalty that is being manifested to the host country or the public. However, the hidden consequence of insider threat in an organization is irreversible compared to the primary consequence of financial loss. In general, an insider is a legitimate user with authorized access to classified information and recognizes the vulnerabilities in an organization's network or system that affect confidentiality, integrity, or availability. Many attacks caused by insiders are more challenging to perceive than those of peripheral invaders whose footprints are harder to assail [5]. In addition, an elevated tendency has been sensed in recent years for unintentional insider threats [6]. Therefore, the motivation for dealing with insider threats is very high and is likely to grow.

Understanding the threat landscape in the knowledge of insider threat is a required concern in a literature review. Several researchers have made various attempts to examine this field in recent decades. Unfortunately, the existing literature experiences numerous shortcomings and requires an updated, more extensive survey in the insider threat field. To illustrate the comprehensive nature of a survey, some focus primarily on the detection mechanism [7–9], which restricts an organized approach to categorize literature [10]. The main objective of this study is to accompany an expansive literature survey in an area of insider threat in a systematic manner, with respective knowledge and research conducted in this field. Since security practitioners and researchers require exploratory defensive solutions for targeted business problems, this study aims to systematize existing defensive solutions in an area of insider threat.

1.1. Survey approach

The main objective of this study is to address the identified limitations in the present research and consolidate them in a more prevalent and contemporary literature study. It emphasizes review and consolidated taxonomies to categorize the literature in a systematic mechanism. In addition, an updated bibliography from the previous survey is revised to ensure relevant work being addressed consistently among the top 100 best-ranked papers in the field of insider threat since 2005 from Google Scholar. Moreover, the topmost cited papers are retrieved from Web of Science databases based on the research topic. Altogether, our retrieved sample research set contains 350 works, and 150 should have been addressed, which fails to satisfy the most relevant criteria. The critical requirement of this survey is to select the most relevant research paper in terms of a year, citation, and problem domain that reviews existing state-of-the-art approaches and categorizes them based on various criteria among a wide range of research in the field of insider threat.

Survey Scope. The broad scope of a present survey in the field of insider threat is based on the following criteria: (a) The articles included in this survey were selected based on the domain of insider threat problem, including definitions, taxonomies of insider threat, analysis and modeling of defensive solutions in terms of detection and mitigation mechanism aligned with a relevant feasibility study. (b) Since this survey's primary focus is an insider threat problem, articles tangentially relevant to an insider threat problem, including masquerade detection approaches, are excluded. (c) The article authored by the same group with similar state-of-the-art methods across multiple papers is ignored. Meanwhile, papers are only included if the latest version of a study that derives limited information from an older version of the study is included in this survey. Based on a scope of survey as guidelines on analysis, the latest literature is studied in an iterative process that categorizes the literature review for finding research articles in a particular field. While processing the papers with the constraint of survey scope, information, including several abstracts, proposed workflow, and bibliography, is identified and categorized according to the proposed study. It contains a review of datasets, incidents, analysis and modeling of practical solutions for detection and mitigation mechanisms, and challenges encountered concerning the best practices. However, the proposed categorization provides valuable insights to classify works in the literature, thus allowing researchers to recognize appropriate relevant work.

1.2. Contribution

This article presents a novel insider threat survey that includes well-versed, comprehensive, concise, and easy to understand for researchers looking for specific information in a broad area. In this study, the significant contributions are summarized as follows: (a) Categorizing varieties of insider threat studies systematically to enable readers to acquire a panoramic interpretation of this diverse topic. (b) survey prevailing taxonomies on insider threat problems, and anticipating a practical and amalgamated taxonomy used for classification: (1) Incident on insider threat, or (2) specialization/coverage of a defensive solution for detection and mitigation mechanism. (3) Collective information of publicly accessible benchmark datasets utilized for evaluating existing detection mechanisms and contrast to other studies is comprised in this survey. (4) Identify existing challenges in insider threat detection and mitigation for auxiliary research directions.

Some of the notable potentials of above specified proposed taxonomy and categorization framework are specified below: (i) easy to acquire domain-specific knowledge for budding researchers, (ii) it is flexible for researchers to identify and pinpoint the shortcomings by reviewing various categories of insider threat based on their empirical behavior in cybersecurity, (iii) In contrast, it is also effective in providing the association of ideas to overcome the existing challenges specified in proposed taxonomy.

The paper is structured as follows. Section 2 elaborates on previous research with their contributions, limitations, and originality exists in their research. Section 3 discusses existing definitions and taxonomies. In Section 4, the past research concerning an insider threat problem is categorized and discussed. An explicit characteristic and subdivision of target major categories are organized as follows: Section 5 deals with incidents and datasets, Section 6 analyzes the incidents, and

Section 7 summarizes defensive solutions in detection and mitigation mechanisms. Section 8 discusses the challenges encountered. Finally, the paper is concluded with further possible directions in the field in Section 9.

2. Existing surveys

This section discusses a summary of previous research and surveys on insider threats, along with a unique proposed taxonomy that is different from previous research.

An ancient taxonomy of malicious threats was first developed by Wood, who classified them based on characteristics of job and attack, hidden motivations, and behavior. Subsequent taxonomies are evolved by modifying the principal taxonomy involving mobile attack characteristics. However, a taxonomy of malicious insiders is divided into two broad categories based on their behavior characteristics in the target system: traitor (or malicious) and masquerader (or compromised) [9]. Further, the enhanced taxonomy of insider threats is three in total, along with careless (or unintentional) perpetrators [11].

The existing literature on insider detection is reviewed, and the research is categorized into three types of approaches: (a) client-based user profiling approaches, (b) third-party level approaches, and (c) service provider-based approaches. Accordingly, service provider-based and third-party level profiling might have a higher chance of recognizing traitors. Client-based user profiling has less chance of identifying traitors. Meanwhile, masqueraders and careless perpetrators are difficult to recognize using all three approaches. The research is categorized in terms of combined psycho-social behavior with technical activities that include the combination of sociological, organizational, psychological, technical, and socio-technical [12]. However, relevant works are segmented into five categories irrespective of insider behavior: biometric-based, cyber activity-based, physiological behavior-based, physical behavior-based, and others [13]. Top trends such as indicator-based, behavioral-based, and artefact-based are considered for detection methodologies using risk analysis [14]. The authors categorized the research based on mitigation strategies in the field of insider threat into six classes in terms of strategies used in prevention itself [15]: (1) physical biometric-based, (2) behavioral biometric-based, (3) physiological biometric-based, (4) host-based asset metrics, (5) network-based asset metrics, and (6) combined asset metrics. The authors discussed critical challenges in malicious insider threat detection and mitigation mechanisms from the big data perspective, stated trends in the field, and provided best practice recommendations for future research. The author summarized the available dataset utilized for insider threat detection mechanisms based on previous research.

2.1. Comparison with our survey

The previous literature review focuses on categorizing diverse studies that include a systematic review of threat detection mechanisms [7–9,11,16]. There are minimal research characteristics based on domain-specific detection and mitigation mechanisms: *insider threat detection approaches* [8,14], and *insider threat prevention approaches* [17]. Our primary focus is to conduct a comprehensive survey related to insider threat involving homogeneous studies [10–12,18–20]. Therefore, it is essential to perform insightful categorization based on the workflow of research efforts to make fine-grained categorization per category.

3. Definitions and taxonomies

In this section, the term 'definitions' and 'taxonomies' existing in the area of insider threat are discussed. It includes heterogeneous definitions of insiders and their possessing threats in addition to existing taxonomies are described in short. It contains three categories in consonance with the purpose of insider, such as malicious and unintentional.

3.1. Definitions

The following annotation perceives knowledge of insiders and insider threats. An *insider* is an employee within an organization who utilizes special privileges such as access, trust, knowledge, or security policies. In contrast, *insider threat* is an act of exploiting such trusted privileges to pose a threat to an organization by violating security policies. However, the variation between malicious and unintentional insiders affects the annotation of insider threats irrespective of their actions. Some well-known definitions assume insider threat is a threat influenced by malicious intention [21,22]. However, others fail to distinguish malicious and unintentional insiders but focus on studying both [12,23–26]. Meanwhile, [6] reviewed and defined the knowledge of unintentional insider threats in their study.

3.1.1. Annotation "insider"

An insider is defined as someone with legitimate access to an organization's computers and networks [25]. As per a report from IBM [27], "an insider is a disgruntled current or former employee misusing sensitive credentials intentionally/unintentionally for revenge or/and monetary gain to disrupt business functionalities". The primary aim of insiders is intellectual property filch, disrupting trusted networks, and utilizing previous information stored in mobile removable drives to impulse online fraud [28]. Regarding information security, an insider is a subject specializing in personal information in classified fields. However, another term specifies insider as a permitted user who maltreats their authority in addition to their experience and neighboring acquisition in a secured network can disrupt an organization with substantial impact [29]. Authorized insider access in an organization's constitution is due to the cognizance of network topologies [30].

In contrast, [31] describes anyone enchanting higher authority to implicit computing resources that include computer framework, data, or program in the inconsistent manner of capricious members. [32] categorized insiders based on trust and concluded them as individuals empowering legitimate rights for accessing, representing, or determining regarding organization assets. Regarding security policies for insiders, [33] considered them a trusted entity that delimits the set of rules in such policies. Where, a non-binary approach is required to indicate the degree of insider access and propose an access control mechanism containing a set of rules for obsessing explicit information. Notably, authors are less interested in interpreting the terms legitimate, uncategorized insiders and outsiders. However, authorized access is possessed by both parties in addition to entering security systems based on system characteristics and organization policy. Consequently, [26] represent insiders as external third-party entities such as independent contractors, business partners, former employees, etc.

3.1.2. Annotation "insider threat"

The term insider threat is comprehensively described by [25], saying that insider activities are vulnerable to sensitive information such as data, resources, and an organization's turbulent process. Trusted insider perpetrates harmful activities to an organization that injuriously affects and benefits an individual [34]. People or employees are considered an originating factor of insider threat by [22] with the constraint of exclusive rights to secured information by abusing their authority and resulting in plotting vulnerability to an organization's security policy. Insider threat is determined as a privileged employee who attempts to violate security measures to prompt embezzlement [12]. In addition, conscious exploitation in security networks is considered an evolving factor for insider threat [22]. However, an abusive event in a trusted entity outputs a vulnerable event to security policies by compromising a set of rules considered for insider threats [23]. However, such vulnerable activities cause explicit risk to an organization [23].

3.1.3. Annotation "unintentional insider threat"

An unintentional insider threat is described as a working or ex-employee, general contractor, or business partner by [6] based on the following characteristics: (1) hold consent to an organization's computational network, data or system. (2) never retains malevolent intention in ignorant activities and causing harmful acts. (3) increasing the likelihood of subsequent vulnerability to an organization system concerning confidentiality, integrity or availability. They were also identified as an inadvertent insider threat by [35] for their characteristics of being careless, inattentive, complacent, or under-trained employees unconsciously accessing information systems with proper authorization. However, the trait of accidental inference magnifies private information disclosure inadvertently [36].

3.2. Taxonomies of unintentional insider threat

In this section, the term 'definitions' and 'taxonomies' existing in the area of insider threat are discussed. It includes heterogeneous definitions of insiders and their possessing threats in addition to existing taxonomies described in short. It contains three categories in consonance with the purpose of insider, such as malicious and unintentional.

CERT Derived Taxonomy

The quadra of unintentional insider threat is defined by [37] for privacy rights: the process of developing malware or is developed using socially engineered sensitive information such as phishing attack, rooted USB drive is known as *malicious code*; The act of publishing sensitive records in either online (or Web) or offline (such as fax, mail to an illegitimate recipient) is known as *divulge*; *Coincidental expose to physical documents* is a trait of disclosing adrift, disposed of, or abscond with a non-digital document including paper records; however, possessing digital records that are being adrift, disposed, or abscond with a laptop, CD, external drive is known as *movable device previously owned*.

Insider Typologies

Considering past research, unintentional insider threats are categorized for their negligent and well-defined motivation [38]. The employees are divided into four types based on the risk of data leakage: *underminers*—the act of violating security policies; *excessive opportunistic* – deliberate to evade security mechanisms for more effectiveness, *data leakers, and social engineers*. Some known sources of data leakage include accidental loss of storage drives, secondary data storage to personal PCs, sharing information in public posts, third parties, etc.

3.3. Malicious insider threat taxonomies

3.3.1. Inside corruptor

Considering confidential networks, historical studies show the classification of inside corruptors and distinguish them into three categories in which audit trails misrecognize them, defined as follows. *Masquerader* –an explicit attacker to detour security controls and penetrate into secure systems, or an implicit attacker anticipates possessing targeted credential information to accomplish malevolent activities; *Miscreant attacker*–mishandles trusted privileges with the aim of misuse instead of masquerade; Surreptitious users–an administrator with the potential of knowing, managing, and controlling security makes them hard to inspect. Previous research fails to include actions relevant to outside corrupters in the working environment. Therefore, this study intensely describes the malicious insider threat involving implicit misuse.

3.3.2. Typologies of insider threat

The characteristics of insider threat are classified into three types [39]: *Access embezzlement* – complicated to recognize since insider intent is authorized access with the motive of dishonesty. *Evading security* — the process of bypassing a certain level of defensive mechanism without interruption and aiming to bypass further. *Insufficient access control* – a technical error due to vulnerability or misconfiguration in the access control element.

3.3.3. Insider threat with various types of knowledge

Malicious insider threat is differentiated into two groups based on knowledge acquired [9]: masquerade and traitor. *Traitors* acquire internal security systems by possessing knowledge of working principles and security policy. Since, they are self-centered and ambitious, they perform malignant activities using their retained credentials. In contrast, *masqueraders* possess a minimum level of knowledge as they break in through the credentials of authorized employees and utilize them to accomplish malicious activities on behalf of others. For instance, a sufferer's account is attained by exposing the vulnerability of a secure system. It is noticeable that the characteristics of traitor and masquerader are not entirely dissimilar. The objective of a masquerader is to acquire the user credential information; meanwhile, a traitor aims to utilize them.

3.3.4. Categorization of insider threat in cloud computing

An insider threat in cloud computing is differentiated into three broad groups: *Rogue administrator in service provider* — governs the activities of possible victims or their on-demand resources that might be leaked or exploited for intellectual property theft, financial fraud, or disrupting the reputation of a cloud service provider. *Exploitation of vulnerability in the cloud* — Insiders perform illegitimate activities such as replica exploitation for fraud. *Exploitation of cloud services* — perform disloyal actions despite company policies. It includes deciphering password credentials, data exportation, and DDoS attacks that are hostile to the company. Meanwhile, from a cloud computing perspective, an insider's target is to abscond and abuse cloud services contrary to standard insider threats. The insider threat in cloud computing is categorized into two types [40]: *Cloud provider employed insider* – an administrator who willingly utilizes legitimate privilege to exploit, backup and exfiltrate the hosted client resources such as performing systematic backup to exploit Personnel Identification Information in cloud data storage, VMs, etc., and *organization employed insider* is similar to activities of traitor that result in deploying IT to the cloud.

3.3.5. Classification of organization-hired insiders

Insiders employed by organizations are classified into four categories [41]: *Pure insiders* –daily employees with limited privileges to accomplish designated jobs such as accessing cards, and targeted networks for services. Meanwhile, the case of pure insiders utilizing privileged rights is considered distinct. *Group of third-party personnel* — forming insider associates including general contractors and intrinsic personnel possessing restricted authority involving diverse categories within an organization such as cleaning workers, service members, etc. However, the communication between such insider associates through physical contact with diverse departments results in finding privacy credentials. The chances of rooting key-loggers are higher as they sniff sensitive information. However, *internal affiliate and external affiliate* insiders signify the individuals without justification and authorization to bypass an organization's security. However, family acquittance, friends, and known employees comprise internal affiliate insiders who abuse the sensitive credentials of employees to commit harmful activities. Meanwhile, external affiliates are distrustful individuals extrinsic to an organization obtaining core access to the network, such as utilizing and evading insecure WiFi, and reverse-engineered sensitive information of legitimate personnel.

3.3.6. Categorization of insider profiles

The insider is profiled into two groups with the constraint of activities, presence and character of associates [41]: *Primitive insiders* are the profile of insiders containing specific characteristics, including predators being accused, caught, and offended. In contrast, sophisticated insiders are competent and formidable to capture. Some of the significant characteristics of primitive insides are defined below. (i) They have nominal technical knowledge but experience in diverse job designations. (ii) They are involved in IP theft, and personal curiosity

motivates them. (iii) They tend to ignore the adverse outcomes of their respective actions. (iv) Since they are emotionally high, their unfamiliar activities are subject to suspicion among colleagues. *Sophisticated insiders* have a profile containing the following characteristics: they tend to perform malicious actions in the long term and are considered more threatening compared to primitive insiders. Some vital characteristics of sophisticated insiders [41] are being objective to reach higher designation due to their responsibilities, performance, reliability, diligence and management skills.

3.3.7. Categorization of insider threat level

Insider threat is classified into three levels [41], in accordance with a distinct consequence: *Self-motivated insiders* in level-1 due to their peculiar motive in the form of revenge and considered complacency. In level-2, *recruited insiders* or individuals influenced by third parties are considered and oppressed using monetary or personal hatred. Since, the trustworthiness is less in recruited insiders, the third-party prefers peculiar insiders hooked on the target organization. *Planted insiders*in level-3 contain completely explicit third-party and insiders; both work together to exploit the targeted organization as authorized personnel and perform data exfiltration in the near future.

3.3.8. Typologies of intention

The significant factors influencing insiders to take a path of the dark side discriminated [41] into three groups: *Fiscal* — competitor organizations target the individual with fiscal requirements and bribe them to perform insider threats in a working organization. As a result, they become an enthusiastic insider. *Political* — the disparate political opinion between employee and employer encourages an employee to associate with external malevolent personnel to accomplish detrimental activities. *Personal* — an employee's motive is to either seek past company secrets and utilize them for blackmailing or assemble vulnerable bait to capture new, sensitive, surreptitious information about a company.

3.3.9. CERT profiled insiders

CERT outlines and profiles insider threats into three broad categories [42]: *IT sabotage* – insider exploits IT companies to damage the organization with the help of resentful employees who acquire governing privileges and technological skills. For instance, disgruntled employees place logic bombs and activate them during job termination. *Intellectual property theft* comprises the reconnaissance executed by employees with the knowledge of both technical (such as software developers and engineers) and non-technical (such as salesmen and clerks) to collect sensitive information as perpetrators and utilize it during their termination. For instance, some cases of IP theft include exploiting IP for personal objectives or vending it to competitor organizations. An employee is considered *fraud* owing to illegitimate alternation or hiding the information of the organization for individual advantage, perpetrated and accomplished by primitive employees acquiring non-technical skills. For instance, desk employees with greed who face huge financial complications are encouraged to commit long-term insider fraud and are often assisted by extrinsic organization units. However, they are considered miscellaneous [6] for categorizing literature under such profiles.

3.4. Systematic taxonomy on insiders

This section represents the systematic taxonomy of insiders' behavior based on the above-discussed annotations and taxonomies. The objective of the systematic review is to provide a broad study of existing taxonomies regarding typologies, target networks and characteristics of insiders. It contains detailed subcategorization for a specific threatening insider in a structural manner. The proposed systematic taxonomy in the domain of insiders is illustrated in Fig. 1 based on incidents of malicious and unintentional insiders. The proposed taxonomy is categorized into three groups and is discussed below. *Typologies* – the insiders are classified based on two subgroups such as knowledge-oriented and behavior-oriented. C*haracteristics* of an insider are defined using intention, levels, and profiles as three notable subcategories. *In cloud computing* – the incidence of insider threat remains high in the cloud environment because of various factors responsible for their employment, including cloud provider-employed and organization-employed.

4. Proposed categorization

From determining the annotations and taxonomies to categorize the literature, it is analyzed that failures are encountered in determining defensive solutions of previous research. Thus, in this section, the pivotal focus is to group the existing research in the insider threat domain using the proposed categorization mechanism. The overview of the proposed mechanism comprising four categories is outlined in the subsequent sections below.

4.1. Workflow of research contributions

The study of past research is categorized in accordance with [43] using a grounded theory mechanism that contains five steps to conduct an insightful literature review on insider threat. *Stage one* — Initially, required input specifications such as enclosure/disclosure criteria, suitable data items about the research field, and search constraints are stated. *Stage two* — searching the essential literature in the field of insider threat. *Stage three* — filtering out unessential and similar articles based on titles, abstract, and presence of a forward–backwards bibliography. *Stage four* — instigating fundamental principles for analyzing past research based on grounded theory that comprises a hierarchy of categorization from top, subcategorization, and their integrations. *Stage five* – presents observation and perception in the targeted field.

Furthermore, the major focus of this survey is to represent the categorization of research using proposed contributions that start with incidents and conclude with an available solution. The defensive solution is illustrated for detection, mitigation and prevention in the area of insider threat. Besides, psychosocial behavior is analyzed and categorized to illustrate the incident analysis of insider threat. The study of a dataset concerning insider threat is gathered and categorized to showcase the existing insider threat benchmark data. However, the workflow of the proposed categorization contains four groups described below: (i) *Dataset analysis* describes available synthetic datasets used to evaluate insider threat detection models illustrated to analyze and model insider threat solutions in terms of incident type, which is explained in Section 5. (ii) *Incident analysis* focuses on studying insider threat behavior to model and group threat incidents as well as describing available taxonomy and definition, modeling behavior framework based on insiders' kill-chain path, and their attack indicators. The critical point of this analysis is to identify significant intention by observing trials, which helps model the categorization of reviews based on defensive solutions.

More information about incident analysis is described in Section 6. (iii) In *defensive solutions*, the information regarding existing solutions in terms of detection and mitigation is categorized, including decoy-based solutions and procedural solutions as subcategories. Moreover, this category illustrates the knowledge of defensive solutions, and their area of development is discussed in Section 8. (iv) In Section 9, the challenges faced by existing solutions to defensive strategies are explained as *an analysis of challenges*. In other words, the knowledge of challenges encountered in the field of insider threat while performing detection and mitigation gives insight into enhancing the past solution to provide a novel mechanism in future.

The proposed workflow represents a top-down approach for insider threat categorization, including four subcategories illustrated in Fig. 2. In a dataset-based survey, each category relies on others; the incident

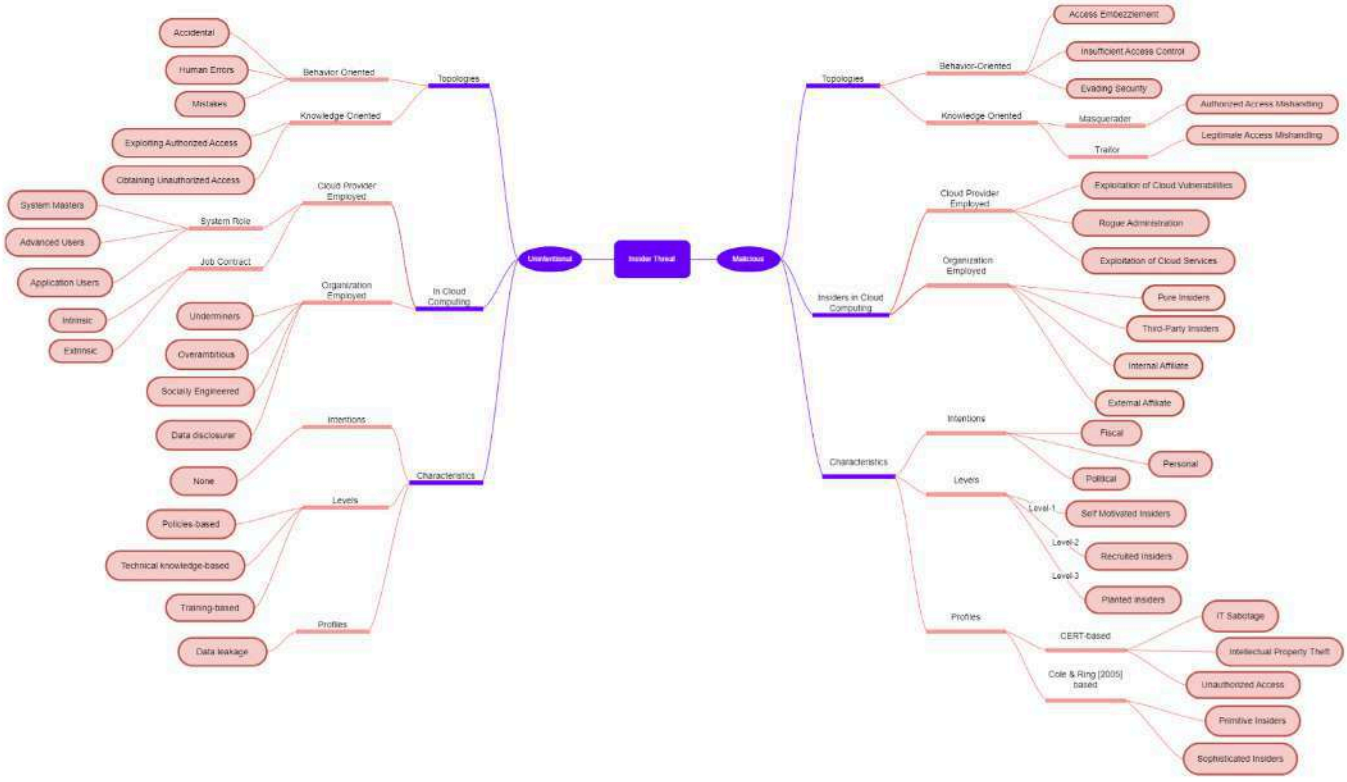

Fig. 1. Systematic taxonomy of insider threat.

analysis intends to review the defensive solution; Meanwhile, defensive solutions utilize the dataset, and incident to interpret the defensive solution; encountered challenges interpret the challenges observed by existing defensive solution.

5. Datasets analysis

Since, a dataset is significant for developing and evaluating innovative solutions in the insider threat field, this section describes appropriate insider threat data and available datasets synthesized in the laboratory or real world. However, it benefits researchers to acquire knowledge on existing insider threat datasets and categorize them based on Fig. 3.

5.1. Datasets

The dataset utilized in the study of insider threat is divided into three categories [44], as represented in Fig. 3: *Masquerader-oriented*, *Traitor-oriented*, and *Assorted malicious*. The following steps are utilized to categorize the literature based on the dataset: (a) differentiating abnormal activity from genuine user activities into two categories, malicious and genuine; (b) when the activity is considered malicious that includes violating policies to access security system with the help of authorized personnel (or traitor-oriented), an illegitimate user (masquerade-oriented) or both (assorted malicious) the cases are compromised in dataset comprehensively. Since this survey's significant focus is recognizing insiders based on malevolent intent, the benign intent branch needs to be more focused and explicitly described in the future. It focuses mainly on a branch of malicious intent in the subcategory of traitors, masqueraders and both in the following section as summarized in Table 1. Notably, research studies are subcategorized into two dataset branches based on per data origin: real-world and synthetic datasets. Since, the only known real-world data is described in [45], this sub-division is used tangentially.

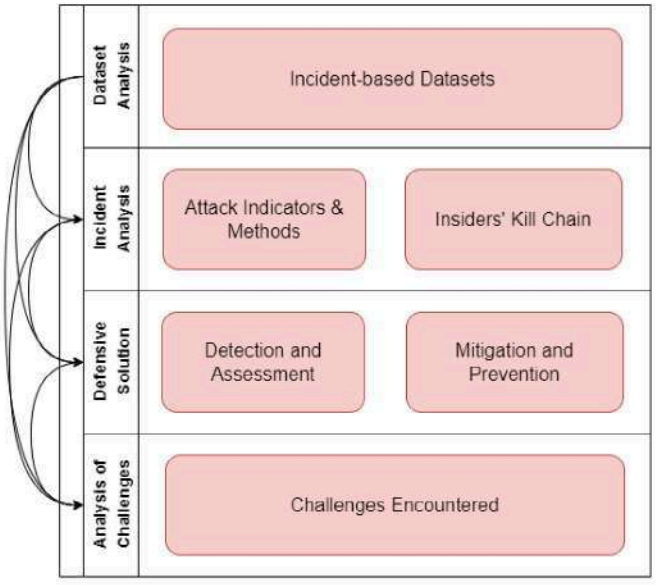

Fig. 2. Workflow of research contribution.

5.1.1. Masquerader-oriented dataset

Regardless of diverse research in the insider threat field to assist, diagnose, and recognize issues of a masquerader, considerable studies have incorporated well-defined synthetic datasets for the detection of masqueraders. However, the dataset comprises malicious patterns in well-formatted data entry, including malicious labels concerning

Table 1
Review on taxonomy of *dataset analysis*.

Dataset	Domain	No. of Subjects	Dataset Details
Windows-Users and Intruder simulations Logs (WUIL) Dataset [46].	Masquerader-oriented Dataset	70 users	File operations such as file open, read, and write
Are You You (RUU) Dataset [47].	Masquerader-oriented Dataset	34 genuine users + 14 masqueraders	Host-oriented activities in numerous PCs.
DARPA 1998 Dataset [22].	Masquerader-oriented Dataset	100 users	network activities and system logs from different PCs
Enron Dataset [45]	Traitor-oriented Dataset	150 users	collective email related activities
APEX 2007 [48]	Traitor-oriented Dataset	8 genuine users + 5 traitors	The activities of users include associated daily log.
CERT Dataset [49]	Assorted malicious Dataset	Approximately 52 users	Log details from web, file, logon, email, external device, psychometric, and LDAP.
TWOS Dataset [50]	Assorted malicious Dataset	24 users	Log details of mouse, network, keyboard and system monitor

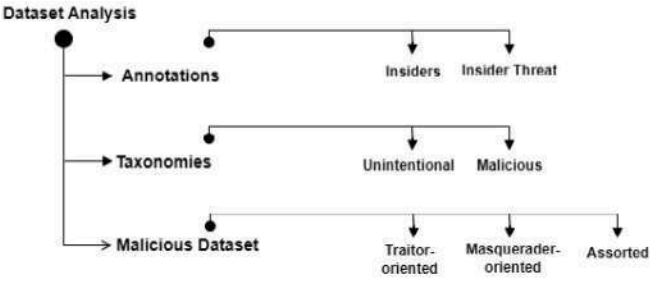

Fig. 3. Detailed categorization of *dataset analysis*.

respective malicious scenarios that target to violate unauthorized access in the form of policies.

Windows-Users and Intruder simulations Logs (WUIL) Dataset.

The dataset incorporates collective file system activities irrespective of different file operations such as file open, file read, and file write [46]. This dataset describes file operation gathered from a maximum of 70 users [46] observed in diverse time intervals when performing daily activity. However, some users spent roughly an hour evolving log activities; others generated log information over several weeks. Nevertheless, the intrinsic tool is used to gather log information containing system audits in diverse versions of Windows machines. Thus, batch scripts are used to simulate masquerade sessions using three categories of skilled users: standard, moderate, and complex, while genuine users are incorporated to gather authorized user log information.

Are You You (RUU) Dataset

A masquerader dataset was gathered from 34 genuine users performing host-oriented activities in diverse PCs, such as admittance of file system, activities, incorporating a library, accessing window registry and system GUI [47]. The description of a dataset comprises a masquerade task performed by 14 humans through limited sessions that locates whether the collected data has fiscal value in either explicit or implicit direction; However, the user notwithstanding any targeted means or resources.

DARPA 1998 Dataset

It is known as the Intrusion Detection & Evaluation dataset, gathered from 100 users from thousands of diverse PCs in a governmental area and artificially created in MIT Lincoln Lab. It applies statistical parameters that solely evaluate and detect enhanced intrusion systems and insider threats [22]. Some information including network activities and system logs, is stored in affected machines, and such attacks are grouped into four categories: DoS attack, Remote access, Root access, and Surveillance. Among the specified categories, the Root access is considered engaging in terms of masquerade-oriented insider threat perception. Due to the evolution of insider threats in advancing technology, McHugh considers this dataset old-fashioned [22].

5.1.2. Traitor-oriented dataset

Compared to the masquerade-oriented dataset, a traitor-oriented dataset is less focused due to the minimal research on traitor recognition. The research solution to masquerade detection must be more complex and unsophisticated, contrasted to traitor recognition [9]. Because, the chance of harmful action carried out by masqueraders is based on victims' inconsistent activity. Alternatively, the probability of copying victims' behavior by insiders including some malicious action is high. This section describes existing datasets relevant to harmful intention of data usage and is considered malicious, focusing on violating policies utilizing authorized access.

Enron Dataset

It contains collective emails gathered from 150 users from Enron corporations [45]. Emails containing external attachments and sensitive details are removed. Text information in these emails is utilized for insider threat detection using text analysis and social network analysis.

APEX 2007

The National Institute of Standards and Technology (NIST) in accord with [48], collected the APEX dataset to focus on simulating the performance of analysts within an intelligence group. The dataset contains activities and associated study reports gathered from 8 genuine analysts; however, five analysts were used to simulate malicious insider activity based on activities of genuine analysts that aim to encounter complex threat detection.

5.1.3. Assorted malicious dataset

The combination of masquerade-oriented and traitor-oriented insider information in a dataset is considered an assorted malicious dataset, and this section is assisted as wide-ranging data for identifying malicious insider activities.

CERT Dataset

The dataset includes collective synthetic information on insider threats [49]. It collects activity information containing log data such as web history, file logs, logon and email data, external device usage, psychometric, and LDAP information.

TWOS Dataset

The dataset was collected through a non-single player game that interacts [50] with genuine companies and produces a synthetic generation of masqueraders and traitors. The game includes six teams with 24 users to play for a week. However, momentary malicious users receive genuine user credentials during masquerade sessions to exploit security machines for approximately 90 min. Meanwhile, during a traitor session, the dataset is collected from fired employees that contains log information of mouse, network, keyboard and system monitor. Besides, the state-of-art features influence the usage of a TWOS dataset in cyber-security [50], affecting insider threat problems that include authorship detection and confirmation, double authentication, and analysis of sentimental data.

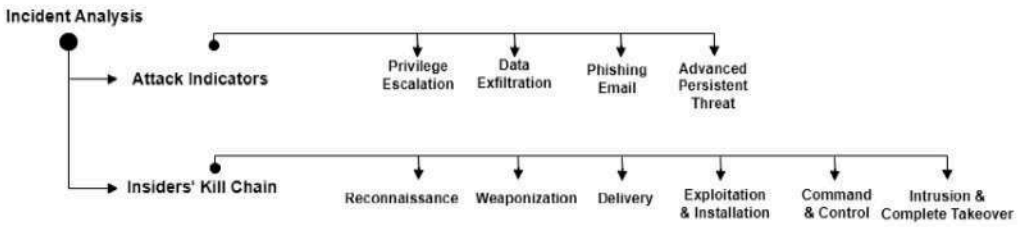

Fig. 4. Comprehensive categorization on *incident analysis*.

6. Incident analysis

The significant factors indicating malicious insider actions while performing harmful incidents are generalized in this section, including relevant research focusing on incident analysis. It comprises attack indicators, techniques, and a kill-chain of insiders for categorization of past research that influences the surveillance of an organization. First, the vital features of insiders to perform an illegitimate operation are considered, followed by the kill-path to compromise a security network, which is studied in this section. In addition, the past research on the incidents of kill chain is analyzed, which assists as a fundamental defensive solution in Section 8. The overview of this categorization is illustrated in Fig. 4.

6.1. Attack indicators and methods

Considering security violations in recent trends, traitors and masqueraders are mainly known for illegitimate access to privileged services depending on attack indicators [51], discussed below. *Privilege escalation*–exploitation of flaws in architecture to by-pass security protocol with the help of two groups: (i) In vertical privileged-escalation, insiders possess sophisticated privileges to perform sensitive operations by attaining kernel-level processes [52]. (ii) In *Horizontal*, an insider exploits the privilege of others by stealing their credentials in critical systems [53] to gain maximum access privileges for himself. It includes sensitive token modification and abuse policies on user accounts for privilege exploitation. *Exfiltration Threats*–Data exfiltration [54] is conducted through unlawful data replication, transmission or recovery in security systems that include covert, tunneled, or overt communication [55] using cloud sync storage such as Dropbox and FTP. It compromises the heart of security components such as confidentiality, integrity, and availability to access and exfiltrate sensitive information [56]. *Phishing emails*–Outsiders perform spear-phishing by mailing authorized employees with the target of infecting them [57]. The goal of an outsider is to detect the generic email addresses of employees [58]. However, email is the basis of phishing attacks originating from information provided by 40% of social website users based on reports of Sophos [59]. *APT* – hijacks the security network using stolen employee credentials and remains passive for a long time to exploit sensitive information [60]. However, an unintentional insider is considered a massive bait to initiate entry points and exploit system administration for massive network access [58]. However, signature-based security products fail to recognize such vulnerabilities.

6.2. Insiders' kill chain

Lockheed Martin adopted six stages to analyze and study intrinsic insider threats as a 'kill-chain' [61], described in this section and presented in Fig. 5. However, terminating threats at any life cycle would disrupt the network architecture. Therefore, the requirement of a defensive solution with respect to every stage of the kill-chain would defend against upcoming primary threats.

Reconnaissance–Insider exploits vertical privilege to search and delegate the classified data for administrative privileges in a targeted network due to their personal curiosity [62]. The companies disclose sensitive information on corporate websites, such as contact information, software information in news magazines, and research information in academic white papers [58], to produce fake documents. Extrinsic attacker cross-checks employee information on LinkedIn with Facebook and manipulates their information [63]. However, the intrinsic threat is hard to recognize. Thus, companies review the polarization vectors concerning insider threat, consider significant entities, and mitigate radicalization bias as a preventive measure. Monitoring information relevant to training, screening time, and log activities is required to detect privacy rights violations and suspect anomalous activities.

Weaponization– Malware software such as Citadel is utilized to gather sensitive financial credentials by exploiting vulnerable spots in targeted organizations to accomplish remote access. The target of an insider is documents containing sensitive information, such as Microsoft Office or PDF, which are prone to infection using APT to bait unintentional insiders through watering holes and spear-phishing [61]. Two-factor authentication is considered to avoid weaponizing [63]. Another form of weaponization is data infiltration due to triggered malware such as BTZ (as Autorun) and spyware in a USB drive connected to PCs in the Department of Defensive infected by Uroburos APT. It focuses on exfiltrating sensitive data in an infiltrated agent's network, which is considered dangerous. In contrast, the insiders can originate from blackmail or extortion but are compromised as a result of a massive amount in return for sensitive data.

Delivery — a process of transferring malware to a targeted network in several steps that is either straightforward Data exfiltration [64] or complicated to possess some resources by acquiring credentials. Data exfiltration incorporates external devices containing malware code into the security network. It uploads it into a personnel network (such as Dropbox) irrespective of intention that aims to teach employees awareness. However, the complicated attack contains intricate steps [65], in which the insider installs malware to steal secretive credentials for accessing the targeted host web service, focusing on exploiting a vulnerability known as web application vulnerability.

Exploitation and Installation — the functionalities of activating, targeting, and exploiting the vulnerability in the target network are accomplished by installing modifiable malware code by incorporating privilege escalation techniques to exploit vulnerabilities [53], focusing on persistent remote access in a security network. Installing such code in an infiltrated system destroys profitable information in central and backup databases and remains unnoticeable [66]. In contrast, authorized personnel with high privilege in a network system may turn into rouge administrators by unconsciously deploying ransomware into the critical system via spear-phishing, which focuses on controlling critical systems.

Command and Control (C2) — The process of controlling the targeted system in a network by a negligent insider in simple traditional infrastructure. In contrast, complex insider threats contain C2 infrastructure [66] to exploit system control and data acquisition interface (SCADA) to destroy industrial control systems. However, the worst-case consequence regarding insider threats in dangerous industrial systems possessing harmful chemicals is nastiest. Another factor affecting critical systems is employee carelessness and becoming bait to

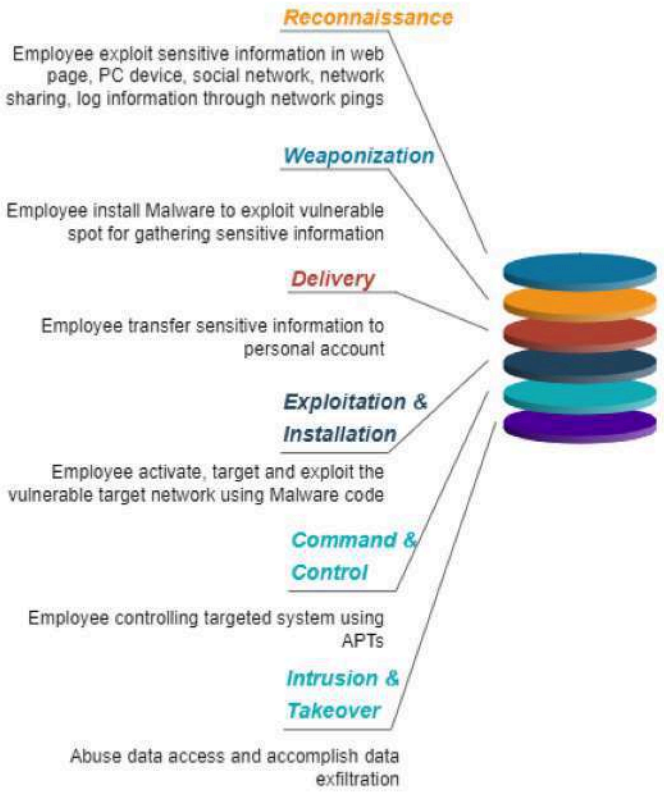

Fig. 5. Path of Insiders' Kill chain.

attackers using APT, which results in possessing sensitive information in a security network using negligent employees' credentials.

Intrusion and Complete Takeover — The main focus of this phase is to accomplish the insiders' objective, which comprises data access and exfiltration, escalation of privileges, or intruding on another target. Since the network system is hijacked at this stage, the possibility of exploiting another vulnerability is greater and more effortless, resulting in seeking other sensitive information. Since, the insider utilizes a combination of technical and non-technical techniques to exploit the targeted organization, the proposed defensive strategies for detecting and mitigating insider threat with respect to every stage of kill-chain is presented in an upcoming section.

7. Defensive solution

This section analyzes the present research study containing detection mechanisms in the insider field. This study includes a comprehensive knowledge of diverse defensive mechanisms and categorizes the study based on insider activities in the existing literature, as illustrated in Fig. 6.

In this section, the studies in the field of insiders are reviewed and categorized into two groups of strategies, such as detection and mitigation, which are discussed in the subsections below. In the detection section, the studies containing state-of-the-art detection methods aimed at detecting malicious patterns are described and categorized in the domain of insiders. Meanwhile, the mitigation section elaborates on the review of recent studies proposing mitigation and prevention of insider threats. However, the sub-classified groups are described below.

7.1. Detection and assessment

This section reviews existing research regarding the proposed state-of-the-art approach for insider threat detection. The study is grouped into five categories with respect to previously mentioned insider threat activities such as biometric, cyber activity, psychosocial, physical, and others. Furthermore, these categories are demonstrated in the subsection below to categorize the insider threat detection studies, summarized in Table 2.

7.1.1. Biometric behaviors

Analyzing biometric patterns such as mouse movement [67] and keystroke typing patterns [113–115] is essential for disrupting insiders in C2 infrastructure. The exploitation of the SCADA system [116] is detected using application-level features.

The biometric activities-based insider threat detection is accomplished using three groups of machine learning techniques as defined below. (1) ***Classification*** — Classification techniques such as decision tree [67], support vector machine [67], Gaussian mixture model [68], Naïve Bayes [69] and probabilistic neural network [67] are suggested for insider detection mechanism to estimate criticality score [69]. Ensemble learning-based classification is beneficial in recognizing insider activities in network access control [113–115] and user command line [117,118] using Lempel–Ziv–Welch (LZW) algorithm. In addition, Bayesian algorithm [70], Bayesian belief network [71] and sequential pattern matching [72] are utilized to recognize insiders, which is also practical for identifying and characterizing *unintended USB channels* [119]. Unique frameworks such as DevEyes [71] and RevMatch [120] analyze historical malware data to detect insiders. (2) ***Anomaly detection*** — keystroke and typing patterns using the local outlier factor algorithm [73] and graph-based anomaly detection [74] to analyze system call features. OCSVM [75] is widely suggested for detecting malicious insiders by monitoring the computation power of GPU cards and the effectiveness of virtual machines.*(3)* ***Clustering*** — an unsupervised ensemble-learning technique for recognizing anomalous system calls in software and resource architecture [70,71,119].

7.1.2. Cyber activity behavior

Insiders often utilize cyber activities rather than physical behavior to possess sensitive credentials through spear-phishing and ransomware to acquire a security network. To find abnormalities, cyber activities such as collective log events, data theft, and network traffic must be processed using machine learning techniques. It aims to disrupt insiders in the process of weaponization, delivery, and exploitation in insiders' kill-chain path. The studies of detection strategies for insiders are subclassified based on the type of event encountered in cyberspace as defined below:

Login events – the collection of login events that occur in cyberspace is considered for insider threat detection using different machine learning techniques. One of the vulnerable cyber events is data theft in clouds' infrastructural resources, which is indeed detected using KNN [76,77], Bayesian network [78] and PROactive Detection of Insider threats with Graph Analysis and Learning (PRODIGAL) [79]. It monitors the data transfer pattern through network messages [76] and critical networks [77]. However, it is essential to secure sensitive credentials such as passwords using elliptic curve cryptography (ECC) [80].

Network traffic – the study that focuses on analyzing the pattern of traffic or packet in network communication for insider behavior modeling in the network layer of TCP-IP protocol [121]. In addition, techniques such as encryption, pattern matching [81,82], XABA-based behavior analysis [83], Bayesian network, dynamic-natured access control [122] and configured dynamic host-protocol [123] are used. It focuses on analyzing network-connected computers [124], gossip protocol for data sharing [125] in mobile devices, and a response mechanism (ISA100.11a) [126] in industrial-based wireless sensor networks are existing detection mechanisms for insiders via random poisoning [127].

Event logs — the study of past research based on features containing event logs such as printers, security, or system logs that are analyzed using the Bayesian theorem to calculate the probability of threat

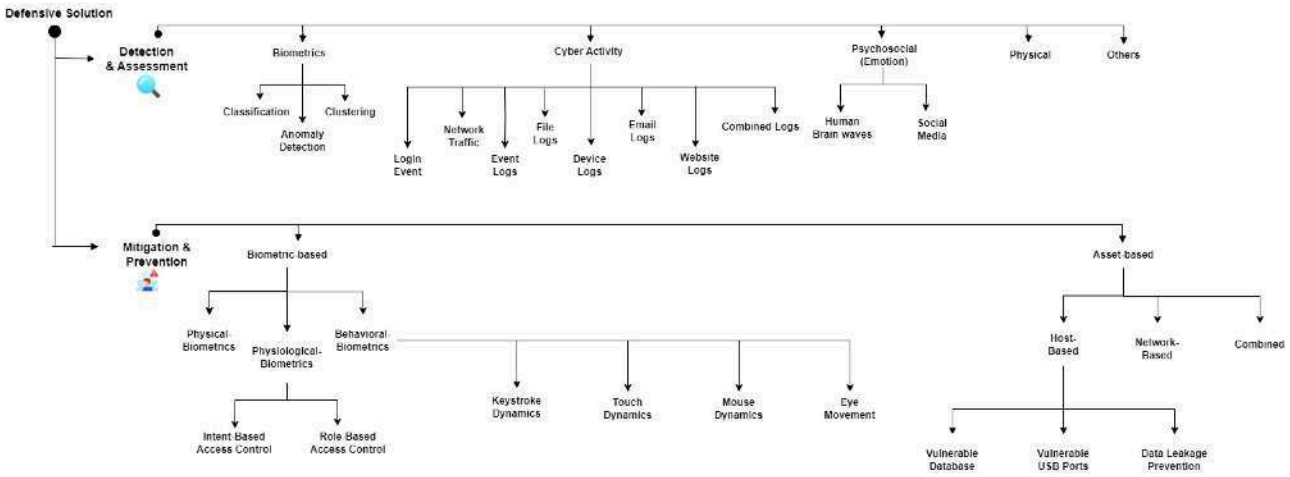

Fig. 6. Comprehensive categorization of defensive solution.

Table 2
Review on taxonomy of *defensive mechanism based on detection solution.*

Defensive Strategy	Behavior type	Activity information	Techniques used
Detection mechanism	Biometric behavior — Classification	Keystroke typing details	Decision tree [67], SVM [67], Gaussian mixture model [68], naïve bayes [69], probabilistic neural network [69], Lempel–Ziv–Welch (LZW) algorithm, Bayesian algorithm [70], Bayesian belief network [71], sequential pattern matching [72] for classification
Detection mechanism	Biometric behavior — Anomaly detection	Keystroke typing details	Local outlier factor algorithm [73], graph-based anomaly detection [74], OCSVM [75]
Detection mechanism	Biometric behavior — Clustering	Keystroke typing details	Local outlier factor algorithm [71]
Detection mechanism	Cyber Activity Behavior-Login Events	Collective log events	KNN [76,77], Bayesian network [78], PROactive Detection of Insider threats with Graph Analysis and Learning (PRODIGAL) [79], elliptic curve cryptography (ECC) [80]
Detection mechanism	Cyber Activity Behavior — Network traffic	Network traffic or packet logs	Pattern matching [81,82], XABA-based behavior analysis [83], Bayesian network
Detection mechanism	Cyber Activity Behavior — Event logs	Event logs from printers, security, or system	Bayesian theorem [84], Rule-based learning [85], hierarchical task segmentation [85], and Markov model [85]
Detection mechanism	Cyber Activity Behavior — File logs	File open, File close, Database queries	Sequential rule mining [86], cryptographic-based watermarking [87], file re-encryption [88], pattern scoring [89], naïve bayes, random topic accessing [90], business process mining [91], and graph analysis [91].
Detection mechanism	Cyber Activity Behavior — Device logs	Memory access logs	PCA, semi-supervised techniques, pattern outlier factor, Bayesian-based trust mechanism [92], combined fuzzy multi-criteria approach [93], hidden Markov model [93], and Baum–Welch technique [93].
Detection mechanism	Cyber Activity Behavior — Email logs	Chat conversation or emails containing texts	Random forest [94], anomalous topic extraction [95]
Detection mechanism	Cyber Activity Behavior — Website logs	Upload and download information	LSTM [96], behavior rule analysis [97], Markov model and virtual honeypot [98]
Detection mechanism	Cyber Activity Behavior — Combined logs	Combined log files from multiple sources	LightGBM [99], XGBoost [100], PCA+kmeans [101], KNN+RF [102], Variational Auto Encoder (VAE) [103], Deep AE [104], SOM [105], HMM [105], CNN + LSTM [106]
Detection mechanism	Psychosocial Behaviors	Behavior in social networks, emails, and website visits	Power spectrum analysis [107], word count analysis [108]
Detection mechanism	Physical Behaviors	Door usage and network traffic	Effect analysis mechanism [109], effect analysis mechanism
Detection mechanism	Other Behaviors	Nonverbal, and biometric information activities such as stylometry	Reactor risk mechanism [110], text analysis [111], gated recurrent unit [112], skip-gram [112]

events [84] for insider detection. Rule-based learning, hierarchical task segmentation, and the Markov model help analyze audit and directory logs [85].

File logs — Relational framework-based community anomaly detection [128], sequential rule mining [86] and cryptographic-based watermarking [87], respectively for insider profile modeling using database and file log information. In contrast, file re-encryption [88], pattern scoring [89], Naïve Bayes, random topic accessing [90], and incremental algorithms are considered for probabilistic approach and consensus clustering insider detection. Data loss prevention methods [91], such as business process mining, graph analysis including knowledge-dependency graphs, and neural dependency, were used to analyze database queries [129].

Device logs — Multiple features of device log information, such as memory access logs, are studied and analyzed using PCA, semi-supervised techniques, pattern outlier factor, and Bayesian-based trust

mechanism [92] for analyzing the performance of VMs [93]. In addition, a combined fuzzy multi-criteria approach, hidden Markov model, and Baum–Welch technique are utilized for device misuse detection.

Email logs — This subsection categorizes past studies based on emails or text in chat conversations for insider threat detection. Widely used techniques include random forest [94] and latent-based semantic indexing for anomalous topic extraction [95] in documents such as credit card numbers and email addresses. Disk forensics is possible by monitoring content using a Google-based rapid response framework.

Website logs — The features of web log information such as upload and download in insider detection mechanism using a two-phase machine learning system, two nonspecific reputation-establishment techniques, and enhanced Long short-term memory (LSTM) [96]. In addition, intelligent grid-based behavior rule-based analysis [97], Markov model and virtual honeypot-incorporated fog computing [98] are advantageous for malicious device detection.

Combined logs — Past research [130] focuses on combining and analyzing log files from multiple sources that can be integrated into homogeneous records for insider detection including device, files, logon, HTTP, and email, using statistical and machine learning techniques [131]. Techniques such as LightGBM [99] and XGBoost [100] analyze and model daily user behavior, which is considered to detect deviated malicious activity. However, boosting algorithms provide a better performance yet require extremely imbalanced data in the case of threat detection with the most genuine behavior considered the most challenging. However, only some others presented a hybrid solution for building genuine user behavior models to recognize anomalous malicious threats. A two-phase detection framework containing the combination of PCA and kmeans [101], KNN and RF [102] are aimed at detecting acquainted high-profile and unacquainted low-profile insiders.

In contrast, authors in [103–105] suggested deep learning techniques for combined insider threat detection that include Variational Auto Encoder (VAE) [103], non-complex DNN, Deep AE [104] with sophisticated hidden layers and best performing Self-Organizing Maps (SOM) [105]. It aims to analyze a large volume of daily cyber activities to build genuine activity signatures. In addition, HMM is considered for modeling users to detect malicious patterns [105]. Recent studies focus on analyzing textual information such as email and website visits. Since, masqueraders perform spear-phishing intending to gather credentials to access a security system [106]. The text information of insiders is converted into 3D information and modeled using CNN and LSTM for insider threat detection using double-layer architecture [106].

7.1.3. Psychosocial behaviors

According to [132], the studies concerning psychological activities in social media in the field of insider threat are approximately minimal and are discussed in this subsection. The author proposed the detection architecture incorporating psychological profiling-based anomaly detection that analyses behavior in social networks, emails, and website visits. Some well-known insider detection strategies include power spectrum analysis in EEG data [107], intent-based access control, and the detection of intrinsic data leakage systems for analyzing *brain signals* to recognize emotions, such as tension, agitation, and anxiety. On the other hand, [108] uses linguistic queries to analyze word count and assess self-centered pessimism and intellectual processing. In social media, user cyber activities such as comments and status updates from Twitter and Facebook are presented based on theories of social bond and situational crime mitigation [133] related to opportunities and activities [134].

7.1.4. Physical behaviors

This section reviews the studies focusing on physical and cyber protection activities concerning security systems using features such as door usage and network traffic, which are analyzed using a combination of large language models. Using an ontological framework to track door access [135] by analyzing door features [109] using an effect analysis mechanism for detecting insider threats in a physical system. Multiple log files from diverse sources such as email, HTTP, and multimedia cameras are analyzed using Euclidean distance [127] to identify malicious nodes.

7.1.5. Other behaviors

This section discusses features with respect to other user activities that differ from psychosocial, cyber, physical and biometric activities or a combination of activities. It includes vulnerability assessment analysis of business operational activities such as Material Control with Accounting (MC&A) using reactor risk mechanism incorporating a combination of human reliability and probabilistic analysis [110]. The combination of aggregation and data consistency [136] technique is proposed for handling communication redundancy and detecting false aggregate information. In contrast, decision-level fusion comprises text analysis for stylometry, web browser activities, and usage patterns that examine biometric and cyber activities [111]. In addition, it combines daily nonverbal and biometric information activities in CERT log files [112] for anomaly detection and data monitoring using a gated recurrent unit, skip-gram, and novel framework [137] for resource and user authentication.

7.2. Mitigation and prevention

The significance of insider threat detection after encountering a substantial loss is considered unremarkable, making the need for mitigation strategies in the field of insiders. In this section, the studies based on mitigation strategies for insiders are reviewed concerning the solution domain and categorized into two groups, Biometric-based and Asset-based, which are summarized in Table 3.

7.2.1. Biometric behaviors

In the case of an insider, as a privileged human without using malware software, a biometric-based solution is employed to mitigate threats by analyzing user biometric behavior and detecting fraudsters. Biometric behavior including physical, physiological and behavioral information such as brain waves, keystroke and eye behavior, and physical body movement, is considered to authenticate a user against fraudsters [160]. The biometric-based solutions are subcategorized into three groups: *physical-biometric, physiological-biometric, and behavioral-biometric, as* defined below.

Physical-Biometrics

This section disrupts the process of data leakage in network systems and prevents them from using human-centric characteristics in the area of insider is well-considered. The evolution of biometrics starts from physical-biometrics including iris, facial recognition, and fingerprints to physiological biometrics, such as brain waves. Physical biometrics is a mitigation strategy since it obtains high accuracy for differentiating one person from another based on their uniqueness [138]. However, the major limitation is that attackers utilize advanced technology to imitate targeted user's physical features. Software like mock fingers [161] and complicated 3D video software are used to attack fingerprint sensors and facial recognition sensors, respectively. Although physical biometrics are practical in user authentication, the studies based on physical features as a mitigation strategy for insider threats are insignificant. Especially in a masquerader-oriented insider threat, the mitigation strategy turns itself into a vulnerable spot where attackers exploit it using illegitimate access. As a result, the mitigation strategy based on physical-biometric should comprise continuous authentication that utilizes biometrics such as eye iris or facial outline for insider verification during the session.

Physiological Biometrics

The physiological behavior such as digital assets in the form of credentials, is something the user has and is utilized and incorporated

Table 3
Review on taxonomy of *defensive mechanism based on mitigation solution.*

Defensive Strategy	Behavior type	Activity information	Techniques used
Mitigation mechanism	Physical biometrics	Iris, facial recognition, and fingerprints	User authentication [138]
Mitigation mechanism	Physiological biometrics — Intent based access control	Brain signals	SVM [139]
Mitigation mechanism	Physiological biometrics — Role based access control	Brain signals	SVM [139]
Mitigation mechanism	Behavioral biometrics	Keystroke typing pattern	Common Vulnerability Scoring System (CVSS)+SVM [140], CNN [141], Neuro Evolution of the Augmenting Topology [142], RBF kernel-based SVM [143], ensembled DNN using Bayesian voting [144], XGBoost [145], Gaussian mixture model [146], sliding window [146]
Mitigation mechanism	Behavioral biometrics — Touch dynamics	Keystroke in android mobile	K-nearest neighbors + fuzzy logic [147], fusion-based feature selection [148], sequential floating forward [148], MLP-based deep learning algorithm [148], SVM [149], ANN [149] and RF [149]
Mitigation mechanism	Behavioral biometrics — Mouse dynamics	Mouse press, and release	KNN [150]
Mitigation mechanism	Behavioral biometrics	Eye movement — temporal, cornea spatial, pupil diameter and radium	K-Nearest-Neighbors [138] and Support Vector Machine [138]
Mitigation mechanism	Host based Asset	Vulnerable database transactions	Petri nets [151], graph analysis [152]
Mitigation mechanism	Host based Asset	Vulnerable USB packet activities	ZedBoard [153]
Mitigation mechanism	Host based Asset	Data leakage operations in SQL transaction	Security access control [154], freeware data leakage prevention system [155],
Mitigation mechanism	Network based Asset	Network attributes such as IP, applicant type, user, request, and response	Autonomic Violation Prevention System (AVPS) [156], Event-Condition-Action (ECA) policy [157]
Mitigation mechanism	Combined Asset	Geo-context data	Geo-context analysis [138], Resilient Access Control Framework (G-SIR) [158], Blacklist mechanism [159]

in access control methods for successful user authentication. Physiological biometrics is useful in disrupting traitors in a kill-chain path by authenticating users based on digital assets such as brain waves, fingerprints, and tokens to grant rightful privileges. The physiological biometric helps analyze and prevent insiders from accessing security systems by incorporating access control mechanisms. The studies of physiological biometrics for access control mechanisms are categorized into two widely known groups, *intent-based* and *role-based*, in the field of insider threat, which is discussed in this section.

(i) Intent-Based Access Control (IBAC)

The main limitation of an access control mechanism is that the user's trust is inevitable all over the session once access is granted using digital assets [162]. In the case of an insider, once access is granted, the security system is prone to privilege misuse, which is unnoticeable. However, Intent-based access control authenticates the users' integrity without focusing on their privileged identity using physiological factors such as human-centric *brain signals*. It analyses brain signals from a P300-based concealed information test (CIT) and brain computer interface (BCI) to estimate positive intention using SVM based optimal threshold for performing particular behavior that prevents insiders from a security network [139]. In addition, using Emotiv EPOC, a 14-channel wireless acquisition device for electroencephalogram, helps gather brain signals in EEGLAB [162].

(ii) Role-Based Access Control

The majority of limitations in IBAC are categorized into three groups, are discussed in this section with respective studies of role-based access control mechanisms [162]. *Deployment*– Extrinsic factors such as hardware issues affect the deployment of EEG and information on brain signals, which results in inaccurate prediction of insiders' intentions. *Scalability* — since, the present study focuses on dealing with two scenarios of malicious intention in analyzing brain signals. It is considered insignificant when insiders acquire other intentions to access organizations' networks. It can be controlled by incorporating a role-based access control mechanism in IBAC that calculates the level of risk irrespective of insiders' other intentions. *Acceptability* — This issue is encountered while incorporating IBAC using sensors on an individual's head to gather signals by enforcing EEG, making it inconvenient based on trust that affects the productivity of insiders in a secure system.

Behavioral-Biometrics

The studies of behavioral biometrics that analyze the unique behavior of an individual for delivering a particular activity with the aim of protecting a security system against insider threats are discussed in this section. The objective of behavioral-biometrics is to disrupt the process of weaponization in the kill-chain where insiders hijack accounts using stolen credentials and avoid them using human-behavior characteristics is well-known. The highly explored behavioral-biometric including keystroke, mouse, eye movement, and touch dynamics are described below.

(i) Keystroke Dynamics

A two-phase access control mechanism-based user verification using an integrated Common Vulnerability Scoring System (CVSS) and SVM [140] detects and groups masqueraders into low, medium, and high. In contrast, CNN [141] converts typing key patterns into image dimensions using ResNet and AlexNet and further classifies them using PCA and SVM. However, hybrid sensors such as triboelectric nanogenerators and electro-magnetic nanogenerators [163] are useful in providing security against password-based vulnerabilities. Techniques such as Neuro Evolution of the Augmenting Topology (P-NEAT) [142], RBF kernel-based SVM [143], ensembled DNN using Bayesian voting [144], XGBoost [145] is evaluated using Recognition Rate or other novel measures for behavioral keystroke authentication.

Some novel measures include uniqueness [164] and mean-standard deviation [165] to validate a false acceptance rate and were evaluated using Manhattan, Euclidean, and Mahalanobis for anomalous keystroke pattern detection in fixed and free-text authentication. Continuous keystroke authentication [146] incorporating a Gaussian model-based anomaly detector and sliding window using keystrokes for the time being to assess online users using FAR and FRR [165]. Another study exploited channel state information collected from user-connected WIFI measurements in [166] for biometric authentication using CNN. Passphrases and keystroke dynamics based on three theories [167] were combined to propose a two-tier user authentication technique. Including Shannon entropy theory (SET), Chunking theory (CT), and keystroke level model that analyses password strength, memorization error and typing error in passwords, respectively, to reduce the false positive rate.

(ii) Touch Dynamics

Several researchers used touch dynamics to develop user biometric verification in Android mobile devices to intercept the process

of weaponization and delivery in insiders' path of kill-chain, which is discussed in this section. A hybrid approach comprising k-nearest neighbors and fuzzy logic [147] for typing behavior analysis of 25 users in touch devices such as Samsung On7 Pro C3590. Meanwhile, a piezoelectric sensor in touch devices [149] helps estimate piezoelectric force using extracted users' touch frequencies for user authentication. In addition, gait and key typing patterns from real-time data are analyzed using fusion-based feature selection [148], sequential floating forward [148], MLP-based deep learning algorithm [148], SVM [149], ANN [149] and RF [149].

(iii) Mouse Dynamics

To highlight unintentional user behavior, the GUI-based user interface using specific commands is insignificant. However, extrinsic factors such as user behavior and physical activities are considered to analyze such unintentional insider activities. Unintentional activities using physical input devices such as a keyboard and mouse to determine insider's physical characteristics [150] are analyzed using random forest for anonymous user detection with respect to age and gender.

(iv) Eye Movement

This section studies the features of eye movement to authenticate the user in the field of insider threat. Eye movement features, such as gaze features unique for each user, are analyzed and discriminated using k-Nearest-Neighbors [138] and Support Vector Machine [138] to detect masqueraders against genuine users. Each user produced 21 gazial features, including temporal, cornea spatial, pupil diameter and radium, etc., with five different scenarios.

7.2.2. Asset-based metrics

This section studies the asset-based approach in insider threat prevention, categorized into three groups: *host-based, network-based, and combined*, are described below.

Host-Based

Some of the significant digital assets available in host-based security systems such as databases and USB ports that contain information relevant to intellectual property and customer-sensitive details, require protection against insiders due to vulnerability in case of data modification, data leakage, and vulnerable USBs. This section discusses the related studies in the field of host-based prevention strategies for insider threat mitigation.

(i) Vulnerable Database

According to [168], malicious database detection is suggested to reduce the exploitation of insiders who seek vulnerable databases to perform illegitimate transactions in a security system. The author analyzes the tasks and transactions of every employee to prevent malicious transactions using graph analysis that includes a directed bipartite graph known as Petri nets [151] in the form of nodes and edges. However, this approach is insignificant due to an increased rate of false negatives concerning the number of transactions. In contrast, unauthorized database manipulation is prevented [152] by analyzing a variable 'threshold' regulating the maximum data manipulation level attached to the items in a database using log entries and a dependency graph containing parameters such as number of records, transactions, and dependencies. However, the dependency graph considers the high-priority record critical data items (CDI) to prevent malicious updates.

(ii) Vulnerable USB Ports

Malware attacks from the origin of USB ports are considered the most vulnerable to security systems, and they are prevented using hardware scenarios that contain malware from USB devices that exploit security systems [169]. A platform independent USB board known as ZedBoard [153] analyses and tracks USB packets based on a logic analyzer to gather USB features such as device and vendor ID, number and typology of endpoint. In addition, USB configuration contains descriptors to mitigate malware uploaded by insiders.

(iii) Data Leakage Prevention

Intellectual property leakage is one of the costliest insider attacks that affect an organization's reputation, and a suggestive mitigative measure of read-only access to external devices adapts security access control [154]. It disrupts the process of data exfiltration using a USB write-blocking script to mitigate malicious insiders. Even though this approach is theoretically acceptable, incorporating such an approach in the organization is insignificant in real-world scenarios. In the case of insiders with administrative privileges, the script can be turned off, and utilizing a USB device to copy sensitive information is a considerable limitation.

However, the mentioned limitation is using a hybrid Data Leak framework, including signature-based and anomaly-based approaches to prevent data leakage [170]. This approach is evaluated using a synthetic and real-time dataset from a hospital and a Dutch IT company that contains SQL transactions analyzed to detect malicious transactions carried out by insiders in an organization. In contrast, using a freeware data leakage prevention system [155], an organization's sensitive information prevents data exfiltration via a USB device by monitoring confidential file transactions such as file copying and file pasting in a security system. However, security policy and its criteria are restricted by a system administrator to mitigate data leakage. While, machine learning technique is beneficial in analyzing file transactions and SQL operations, detecting malicious behavior, and blocking such malicious file transactions for upholding confidentiality in a security system.

Network-Based

The popularity and evolution of computer networks induced significant network vulnerabilities, causing insiders to exploit them to gather sensitive information that results in data leakage. However, access privilege restriction is widely considered for mitigating such data leakage incidents without exploiting network-based solutions. Solution based on network analyzes network traffic using Snort to process and extract network attributes such as IP, applicant type, user, request, and response [171]. It is considered a popular mitigation strategy that strengthens information security and privacy in the field of insiders over a network by preventing malicious transactions. One such mitigation approach is the Autonomic Violation Prevention System (AVPS) [156], which utilizes in-line components and autonomic policies to analyze and mitigate such insiders' activities using the Event-Condition-Action (ECA) policy [157]. The performance of such an approach is evaluated using diverse operating systems such as RedHat and Fedora over various network applications, including FTP, Web servers, and databases.

Combined

Apart from host-based and network-based solutions, the insider threat can be mitigated using other strategies, including geo-context analysis based on social media and mobile devices. It analyzes the geo-context data of insiders in a working environment to recognize malicious behavior and deny user access to the security system in an organization [138]. Resilient Access Control Framework (G-SIR) [158] estimates the reliability of insiders by analyzing social network activities. In contrast, a hybrid framework [159] combines two phases of prevention and a blocklist mechanism aims at blocklisting matching against insiders and classifying insider activities based on historical user behavior in the prevention and detection phases. However, countermeasures for insider threats are categorized into three groups with respect to technological, behavioral, psychological, and cognitive policies [172]. *Pre-measure* — mitigation strategies before witnessing a threat against insiders; *Post-measure* — measures upheld after witnessing insider threat and their departure; *While-measure* — measures followed during insider employed in an organization. Since, it focuses on mitigating insider threats and their consequence before an attack encounter, pre-measure is considered effective than others.

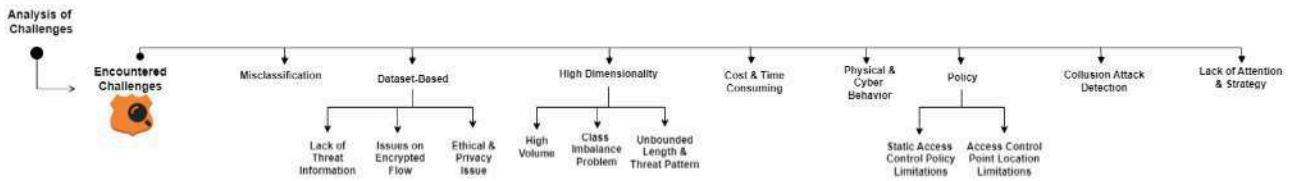

Fig. 7. Comprehensive categorization of defensive solution.

8. Categorization of challenges encountered in detection and mitigation mechanism

In this section, the studies of current challenges encountered in existing research in insider threat detection and mitigation strategies are categorized into eight groups, as depicted in Fig. 7. These challenges are based on misclassification, insider dataset and their behavior types, dimensionality, etc., discussed in the sub-sections below.

8.1. Misclassification

Since insiders are authorized employees, the detection approaches fail to differentiate such insiders as genuine or malicious [173]. Anomaly detection techniques that apply supervised or unsupervised algorithms are commonly utilized for insider threat detection to sense abnormality based on deviations in a genuine behavior pattern and are considered malicious. However, the possibility of genuine activities might result in behavior deviations and, consequently, a false alarm arises that affects the enterprise environment to adopt insider threat detection strategies [117]. Thus, minimizing false positives and negatives while maintaining the accuracy rate of detection strategies is a notable challenge.

8.2. Insider threat datasets

The study of difficulties faced while analyzing and evaluating insider threat detection mechanisms using insider threat datasets is discussed in this section. Some difficulties are the need for more factual threat information, privacy and ethical issues, and analysis errors affecting the performance of detection strategies, which are explained below. (i) *Lack of Threat Information* –Insufficient real-time threat data from an organization affects the performance of insider threat detection methods, drawing the boundary for advanced research in insiders [8, 17,93]. Even though, an artificially created synthetic dataset based on a particular is used by present research, the evolving insider threats are difficult to interpret by detection methods, which is a consequential disadvantage [174]. The available threat data must be updated to contain only a few malicious instances, and analyzing such datasets is considered insignificant. (ii) *Ethical and Privacy Issues* — Since ethical and privacy policies restrict access to sensitive information to outsiders, the organization fails to provide their information for research in the field of insider threat detection. The existing methods apply synthetic datasets to analyze insider detection systems due to the lack of real-insider datasets. However, the absence of real-time insider data makes it difficult for the insider detection system to evaluate and analyze their performance. This increases biases in model prediction [50]. (iii) *Analysis Issues on Encrypted Flows or Encrypted Data Packets* –The rapid growth in technology assists attackers in masking themselves to avoid intrusion detection systems using cryptography. In the case of encrypted data, the detection system filters out such insider behavior and is considered another restriction of the intrusion detection system [81].

8.3. High dimensionality

This section describes the complications confronted while processing and analyzing high-dimensional insider data for detection strategies. *(i) High Volume* — For insider threat detection, the real daily log details are gathered daily to analyze user behavior patterns in the working environment. Since, the size of the log details is enormous, it takes work to analyze the massive volume of employee activities [72, 93,107]. In contrast, organizations need to deal with a large volume of employee behavior to monitor them [69]. As a result, it needs to pay more attention to the prerequisite of manual analysis with the help of auditors and network administrators [72]. *(ii) Class imbalance problem* — Despite the high volume of data used to analyze malicious patterns of insiders, the occurrence of malicious behavior is comparatively less than in normal daily activities. In the case of analyzing user behavior using high-dimensional daily activities, machine learning models consider lesser instances as outliers and neglect them during analysis. The class imbalance problem arose that only analyzed genuine behavior for processing and predicting malicious insider threats. It is one of the most challenging problems affecting machine learning algorithms' performance for insider threat detection [175]. *(iii) Unbounded Length and Threat Patterns* –The log containing diverse heterogeneous activities encounters data analysis problems when analyzing and classifying malicious behavior using high dimensional data [8,131]. Due to changing patterns of malicious activities, supervised algorithms fail to recognize abnormal activity when encountering new malicious behavior. It can be solved using unsupervised learning with a specific volume of data that limits the usage of insider threat detection methodologies [74].

8.4. Physical and cyber behavior

Studies focus on user activity in cyber or physical security systems for insider threat detection, are considered as a substantial limitation of cybersecurity [109,127]. However, according to past research, concerning both cyber and physical security behavior for analyzing insiders is limited [176]. In contrast, the studies concentrate on access control mechanisms to combat unauthorized access of insiders against physical networks. However, it is considered insignificant in changing scenarios of insider threats.

8.5. Costly and time-consuming

Unlike unsupervised learning, supervised learning is the most suitable and approachable for insider threat detection; it learns data to build a model using a classification algorithm. This results in increasing the training process with essential homogeneous log entries in the area of insider threat detection. It affects the cost and time for model training and execution when orchestrating applications for insider threat detection [118].

8.6. The policy

In an organization, the employee is well aware of policies and practices being followed. Policies aim to regulate insiders' privilege to a security system that aims to uphold regulations using access control policies. Such policies regulate the privilege of activities such

as reading, writing, and execution of processes using the trustworthiness of legitimate users. In contrast, a privileged insider focusing on malicious intentions might destroy sensitive information [74]. Insiders such as rogue, oblivious, pseudo-malicious, and hostile may exploit access rights to abuse the security system [177]. However, enterprises encounter the above-mentioned threats more often in the absence of an access control mechanism [162].

Limitations of Static Access Control Policy — The existing studies incorporate fundamental static policy for designing access control techniques using crypto-credentials as attributes. Some of the vulnerabilities in static access control policies include changing the behavior of legitimate users, under version credentials, and modifying document structures that are unrecognizable by access control policies [178]. *Limitations of Access Control Point Location* — Since the access control policy focuses on disrupting insiders' threat, the policy is vulnerable and might exploited by malicious outsiders, remaining challenging. In addition, the deployment nature of access control applications against insider threats in a network is another challenge. The peculiar spot for installing such an access control mechanism in a network remains thought-provoking [122].

However, the above-mentioned challenges are tackled in existing research based on multi-step strategic frameworks and dynamic usage control policies that provides significant contribution in access control mechanism are included below. The Multi-step operations strategic framework [179] suggests three verticals to reduce risk in cloud organizations. It comprises identification and prevention, securing operations, detection, and response. In identification and prevention, operations such as interface monitoring, Anti-Virus software, and Anti-Phishing are performed to detect and prevent malicious behavior. Meanwhile, securing operations such as employee training, intrusion detection systems, audits, and password security is encompassed in the computer systems of working employees in an organization to analyze and detect malicious behavior. However, the detected malicious activities are processed in the final stage of detection and response, comprising backup and restore operations, insurance and planning offline essential services.

On the other hand, safety decidable models are analyzed based on attributes of objects (or domains) in usage control authentication models using safety decidability [180] for pre-authorization, known as $\text{PreUCON}_{\text{A}}^{\text{Finite}}$. Where, attribute domains contain infinite object identifiers along substantial restrictions. In contrast, in [181], the open challenge of undecidable safety while combining infinite attributes with single finite attributes domain along limited restrictions is formulated to address the question of safety decidability.

Meanwhile, one of the usage control authorization approaches applies a verification tool based on formal property [182] using Rhapsody software. The security requirements of usage control are represented in the property specification of the dynamic verification tool with an aim to analyze every action generated in each phase of the application being executed. In contrast, limitations such as concurrency and model left issues [183] in the usage control authorization model are handled to achieve a synchronized usage control process. It is further verified by applying the SPIN model checker [184], a verification tool to evaluate the correctness of the concurrent usage control authorization model. However, one method to evaluate the correctness is to gather and analyze protection states in end-to-end correctness verification.

As a result, the evolving cloud adopted technology in an organization setting requires updated policies for significant access control mechanism to combat unauthorized access.

8.7. Collusion attack detection

The existing studies aim to recognize solitary insider detection and need to focus on collaborative insider threats comprising two or more insiders; It is considered hard to recognize. The major limitation of collusion insider threat is that combined activity results in malicious action while it is considered benign when analyzing separate activities. Further research is required to concentrate on collusion threats, which is necessary [185].

8.8. Lack of attention and strategy

Despite existing studies concentrating on insider threats [72], the organization emphasizes outsiders. However, in the area of cybersecurity, the authors detected various security issues. In contrast to organizations, researchers consider malicious insiders more harmful than extrinsic outsiders. In addition, the limitations of the characteristics of malicious insiders are based on intention and strategies [68]. Since detection strategies applicable in a lower layer of a security system, such as data mining in a host-based machine, affect the particular threat pattern or scenarios, they are indeed pre-emptive. The present study estimates that past research on malicious insiders seems lacking and defective in detecting and preventing such insider threats.

9. Conclusion and future works

This study aims to provide a structure of research information in the field of insider threat, with the help of past theories, for a comprehensive literature review. It illustrates four major classes for research categorization, as illustrated in Fig. 2. They are (1) the study on available artificial datasets utilized by past research in the field of insider threat, which is categorized and described to evaluate existing solutions. (2) An incident analysis correlates the review on possible indicators of insiders, including taxonomy and definition to accomplish an attempt of attack using insiders' path of kill-chain. It is beneficial in categorizing defensive solutions for insider detection based on observed trails in the kill-chain path. (3) The available defensive solution is reviewed and categorized into two groups: (a) detection and (b) mitigation strategies. Studies of defensive solutions regarding the vital area of insider threat are discussed with a focus on annotations and taxonomies. (4) The proposed taxonomy includes categorizing challenges encountered and defining them concerning defensive solutions incorporated against insiders.

Some of the observations are highlighted in the following section to enhance future research in the area of insider threats:

- According to [9], real-time insider behavior is considered a significant limitation in evaluating insider threat detection research. However, only some existing synthetic datasets help evaluate detection strategies that comprise instances of malicious behavior and are not incorporated into a real working environment. Thus, the need for a dataset is a significant challenge for researchers to use the proposed methodology in insider-based case studies in working environments.

- The knowledge of detection strategies based on goal-oriented features is highlighted while ignoring motivation and their capabilities. The characteristics of insider motivation include privacy issues and datasets corresponding to psychosocial features and decoys. It derives insiders' capability based on present data. However, it is required to include the above-mentioned characteristics in an existing dataset to evaluate detection methods against insider threats.
- Biometric or multifactor authentication helps defend against malicious insider threats and mitigate the malicious insiders against security systems. For biometric behavior authentication, RNN is helpful in recognizing genuine user behavior.

- The existing research focus on malicious insiders that fails to analyze and detect unintentional insiders is a significant challenge in a working environment. Since the occurrence of unintentional insiders is higher than malicious insiders, the need for detecting unintentional malicious insiders is required in future research.

- Since, the increased studies in anomaly detection deal with class imbalance issues in a dataset. However, it is solved by reviewing and incorporating the best-performing sampling technique, which is applicable in existing research that deals with imbalanced datasets in anomaly-detection techniques. In addition, the balanced dataset is modeled to recognize malicious insiders.

The last recommendation is to utilize natural language processing for analyzing email phishing, which malicious insiders or external outsiders inject to recognize malicious emails. It can be achieved using the BERT model for the classification of emails into either malicious or non-malicious emails.

CRediT authorship contribution statement

Asha S.: Writing – review & editing, Writing – original draft, Visualization, Validation, Software, Resources, Methodology, Data curation, Conceptualization. **Shanmugapriya D.:** Writing – review & editing, Supervision, Project administration, Investigation, Formal analysis.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Asha S reports equipment, drugs, or supplies was provided by Avinashilingam Institute for Home Science and Higher Education for Women.

Data availability

No data was used for the research described in the article.

Uncited references

[186]

Acknowledgments

The Centre for Cyber Intelligence under DST CURIE AI Phase II Project at Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu, India is acknowledged for providing infrastructural facilities for this research.

References

[1] Forbes, Top cybersecurity predictions, 2023, https://www.forbes.com/sites/emilsayegh/2022/12/15/top-cybersecurity-predictions-2023/?sh=36224e8c383f. (Accessed 22 February 2023).
[2] Cyber Security Hub, The biggest data breaches and leaks of 2022, 2023, https://www.cshub.com/attacks/articles/the-biggest-data-breaches-and-leaks-of-2022. (Accessed 22 February 2023).
[3] CrowdStrike, 2022 Global threat report, 2023, https://irp.cdn-website.com/5d9b1ea1/files/uploaded/Report2022GTR.pdf. (Accessed 22 February 2023).
[4] Verizon, 2022 Data breach investigations report, 2023, https://www.verizon.com/business/resources/T158/reports/dbir/2022-data-breach-investigations-report-dbir.pdf. (Accessed 22 February 2023).
[5] M. Moore, Cybersecurity Breaches and Issues Surrounding Online Threat Protection, IGI Global, 2016.
[6] M.L. Collins, M.C. Theis, R.F. Trzeciak, J.R. Strozer, J.W. Clark, D.L. Costa, T. Cassidy, M.J. Albrethsen, A.P. Moore, Common Sense Guide to Prevention and Detection of Insider Threats, fifth ed., CERT, Software Engineering Institute, Carnegie Mellon University, 2016.
[7] M. Bertacchini, P. Fierens, A survey on masquerader detection approaches, in: Congreso Iberoamericano de SeguridadInformática, Universidad de la República de Uruguay, 2008, pp. 46–60.
[8] A. Gheyas, A.E. Abdallah, Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis, Big Data Anal. 1 (1) (2016) 6.
[9] M.B. Salem, S. Hershkop, S.J. Stolfo, A survey of insider attack detection research, in: Insider Attack and Cyber Security, Springer US, 2008, pp. 69–90.
[10] A. Azaria, A. Richardson, S. Kraus, V.S. Subrahmanian, Behavioral analysis of insider threat: A survey and bootstrapped prediction in imbalanced data, Trans. Comput. Soc. Syst. 1 (2) (2014) 135–155.
[11] L. Liu, O. de Vel, Q. Han, J. Zhang, Y. Xiang, Detecting and preventing cyber insider threats: A survey, IEEE Commun. Surv. Tutor. 20 (2018) 1397–1417.
[12] J. Hunker, C.W. Probst, Insiders and insider threats: An overview of definitions and mitigation techniques, J. Wirel. Mob. Netw., Ubiquitous Comput., Depend. Appl. 2 (1) (2011) 4–27.
[13] M.N. Al-Mhiqani, R. Ahmad, Z. Zainal Abidin, W. Yassin, A. Hassan, K.H. Abdulkareem, N.S. Ali, Z. Yunos, A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations, Appl. Sci. 10 (15) (2020) 5208.
[14] A. Sanzgiri, D. Dasgupta, Classification of insider threat detection techniques, in: Annual Cyber and Information Security Research Conference, ACM, 2016, p. 25.
[15] R.A. Alsowail, T. Al-Shehari, Techniques and countermeasures for preventing insider threats, PeerJ Comput. Sci. 8 (2022) e938.
[16] S. Walker-Roberts, M. Hammoudeh, A. Dehghantanha, A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure, IEEE Access 6 (2018) 25167–25177.
[17] A. Zaytsev, A. Malyuk, N. Miloslavskaya, Critical analysis in the research area of insider threats, in: Proceedings of the 2017 IEEE 5th International Conference on Future Internet of Things and Cloud, FiCloud, Czech Republic, Prague, 2017, pp. 288–296.
[18] S.M. Ho, M. Kaarst-Brown, I. Benbasat, Trustworthiness attribution: Inquiry into insider threat detection, J. Assoc. Inf. Sci. Technol. 69 (2018) 271–280.
[19] M. Kim, K. Kim, H. Lee, Development trend of insider anomaly detection system, in: Proceedings of the 20th International Conference on Advanced Communication Technology, ICACT, IEEE, Chuncheon-SI Gangwon-Do, Korea, 2018, pp. 373–376.
[20] J. Ophoff, A. Jensen, J. Sanderson-Smith, M. Porter, K. Johnston, A Descriptive Literature Review and Classification of Insider Threat Research, Technical Report, 2014.
[21] N. Einwechter, Preventing and detecting insider attacks using IDS, 2010, https://www.symantec.com/connect/articles/preventing-and-detecting-insider-attacks-using-ids. (Accessed 1 August 2023).
[22] M. Theoharidou, S. Kokolakis, M. Karyda, E. Kiountouzis, The insider threat to information systems and the effectiveness of ISO17799, Comput. Secur. 24 (6) (2005) 472–484.
[23] M. Bishop, Position: Insider is relative, in: Workshop on New Security Paradigms, ACM, 2005, pp. 77–78.
[24] F.L. Greitzer, D.A. Frincke, Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation, in: Insider Threats in Cyber Security, Springer, 2010, pp. 85–113.
[25] S.L. Pfleeger, J.B. Predd, J. Hunker, C. Bulford, Insiders behaving badly: addressing bad actors and their actions, IEEE Trans. Inf. Forensics Secur. 5 (1) (2010) 169–179.
[26] J. Predd, S.L. Pfleeger, J. Hunker, C. Bulford, Insiders behaving badly, IEEE Secur. Priv. 6 (4) (2008) 0066–0070.
[27] [IBM Report 2022] https://www.ibm.com/topics/insider-threats.
[28] L. Flynn, C. Huth, R. Trzeciak, P. Buttles, Best Practices Against Insider Threats in All Nations, IEEE, Physcataway, NJ, USA, 2013.
[29] R. Chinchani, D. Ha, A. Iyer, H.Q. Ngo, S. Upadhyaya, Insider threat assessment: Model, analysis and tool, in: Network Security, Springer, 2010, pp. 143–174.
[30] Q. Althebyan, B. Panda, A knowledge-base model for insider threat prediction, in: Information Assurance and Security Workshop, IAW'07. IEEE SMC, IEEE, 2007, pp. 239–246.
[31] S. Sinclair, S.W. Smith, Preventative directions for insider threat mitigation via access control, in: Insider Attack and Cyber Security, Springer, 2008, pp. 165–194.
[32] C.W. Probst, J. Hunker, M. Bishop, D. Gollmann, Summary - Countering insider threats, in: Countering Insider Threats (Dagstuhl Seminar), Leibniz-Zentrum fuerInformatik, Germany, 2008.
[33] M. Bishop, S. Engle, S. Peisert, S. Whalen, C. Gates, Case studies of an insider framework, in: Hawaii Int. Conference on System Sciences, IEEE, 2009, pp. 1–10.
[34] F.L. Greitzer, D.A. Frincke, M. Zabriskie, Social/ethical issues in predictive insider threat monitoring, in: Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives, 2010, pp. 132–161.
[35] D. Liu, X. Wang, L.J. Camp, Mitigating inadvertent insider threats with incentives, in: Int. Conference on Financial Cryptography and Data Security, Springer, 2009, pp. 1–16.

[36] V. Raskin, J.M. Taylor, C.F. Hempelmann, Ontological semantic technology for detecting insider threat and social engineering, in: Workshop on New Security Paradigms, ACM, 2010, pp. 115–128.
[37] F.L. Greitzer, J. Strozer, S. Cohen, J. Bergey, J. Cowley, A. Moore, D. Mundie, Unintentional insider threat: contributing factors, observables, and mitigation strategies, in: Hawaii Int. Conference on System Sciences, IEEE, 2014, pp. 2025–2034.
[38] D.S. Wall, Enemies within: Redefining the insider threat in organizational security policy, Secur. J. 26 (2) (2013) 107–124.
[39] S.M. Bellovin, The insider attack problem nature and scope, in: Insider Attack and Cyber Security, Springer, 2008, pp. 1–4.
[40] M. Kandias, N. Virvilis, D. Gritzalis, The insider threat in cloud computing, in: Int. Workshop on Critical Information Infrastructures Security, Springer, 2011, pp. 93–103.
[41] E. Cole, S. Ring, Insider threat: Protecting the enterprise from sabotage, spying, and theft, in: Syngress, 2005.
[42] D.M. Cappelli, A.P. Moore, R.F. Trzeciak, The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud), Addison-Wesley, 2012.
[43] J.F. Wolfswinkel, E. Furtmueller, C.P. Wilderom, Using grounded theory as a method for rigorously reviewing literature, Eur. J. Inf. Syst. 22 (1) (2013) 45–55.
[44] A. Harilal, F. Toffalini, J. Castellanos, J. Guarnizo, I. Homoliak, M. Ochoa, TWOS: A dataset of malicious insider threat behavior based on a gamified competition, in: Int. Workshop on Managing Insider Security Threats, ACM, 2017, pp. 35–46.
[45] Enron email dataset, 2015, http://www.cs.cmu.edu/~enron/. (Accessed 1 August 2023).
[46] B. Camiña, R. Monroy, L.A. Trejo, M.A. Medina-Pérez, Temporal and spatial locality: an abstraction for masquerade detection, IEEE Trans. Inf. Forensics Secur. 11 (9) (2016) 2036–2051.
[47] M.B. Salem, S.J. Stolfo, Modeling user search behavior for masquerade detection, in: Int. Workshop on Recent Advances in Intrusion Detection, Springer, 2011, pp. 181–200.
[48] E. Santos, H. Nguyen, F. Yu, K. Kim, D. Li, J.T. Wilkinson, A. Olson, R. Jacob, Intent-driven insider threat detection in intelligence analyses, in: Int. Conference on Web Intelligence and Intelligent Agent Technology, IEEE, 2008, pp. 345–349.
[49] J. Glasser, B. Lindauer, Bridging the gap: A pragmatic approach to generating insider threat data, in: Security and Privacy Workshops, IEEE, 2013, pp. 98–104.
[50] A. Harilal, F. Toffalini, I. Homoliak, J. Castellanos, J. Guarnizo, S. Mondal, M. Ochoa, The wolf of SUTD (TWOS): A dataset of malicious insider threat behavior based on a gamified competition, J. Wirel. Mob. Netw., Ubiquitous Comput., Depend. Appl. (JoWUA) 9 (1) (2018) 54–85.
[51] S. Haggard, J.R. Lindsay, North Korea and the Sony Hack: Exploring Instability Through Cyberspace; AsiaPacific Issues. Vol. 117, East-West Center, Honoloulu, HI, USA, 2015, pp. 1–8.
[52] F. Jaafar, G. Nicolescu, C. Richard, A systematic approach for privilege escalation prevention, in: Proceedings of the IEEE International Conference on Software Quality, Reliability and Security Companion, QRS-C, IEEE, Vienna, Austria, New York, NY, USA, 2016, pp. 101–108.
[53] N.G. Tsoutsos, M. Maniatakos, Fabrication attacks: Zero-overhead malicious modifications enabling modern microprocessor privilege escalation, IEEE Trans. Emerg. Top. Comput. 2 (2014) 81–93.
[54] C. Janssen, Data exfiltration, in: Techopedia, 2015, http://www.techopedia.com/definition/14682/data-exfiltration. (Accessed 28 April 2023).
[55] A. Giani, V.H. Berk, G.V. Cybenko, Data exfiltration and covert channels, in: Proc. SPIE, 2006, p. 6201.
[56] J. Clark, S. Leblanc, S. Knight, Risks associated with USB hardware Trojan devices used by insiders, in: Proceedings of the IEEE International Conference on Systems Conference, SysCon, Montreal, QC, Canada, 2011, pp. 201–208.
[57] L. Cleghorn, Network defensive methodology: A comparison of defensive in depth and defensive in breadth, J. Inf. Secur. 4 (2013) 144–149.
[58] C. Pernet, APT kill chain—Part 3: Reconnaissance-airbus D & S CyberSecurity blog, 2014, https://airbus-cybersecurity.com/apt-kill-chain-part-3-reconnaissance. (Accessed 30 August 2023).
[59] S. Gates, Threat intelligence predictions report, in: NSFOCUS 2017, 2017, http://blog.nsfocusglobal.com/wp-content/uploads/2017/02/TI-2017_Predictions_Report_v4.pdf. (Accessed 2 August 2023).
[60] P. Giura, W. Wang, A context-based detection framework for advanced persistent threats, in: Proceedings of the 2012 International Conference on Cyber Security, CyberSecurity, Washington, DC, USA, 2012, pp. 69–74.
[61] E.M. Hutchins, M.J. Cloppert, R.M. Amin, Intelligence-driven computer network defensive informed by analysis of adversary campaigns and intrusion kill chains, in: Proceedings of the 6th International Conference on Information Warfare and Security, Washington, DC, USA, 2011, pp. 80–81.
[62] L. Ray, H. Felch, Detecting advanced persistent threats in oracle databases: Methods and techniques, in: Strategic Information Systems and Technologies in Modern Organizations, IGI Global, Hershey, PA, USA, 2017, pp. 71–89.
[63] J. Scott, D. Spaniel, In 2017, the Insider Threat Epidemic Begins, Institute for Critical Infrastructure Technology, 2017, https://icitech.org/wp-content/uploads/2017/02/ICIT-Brief-In2017-The-Insider-Threat-Epidemic-Begins.pdf. (Accessed 14 August 2023).
[64] J. Kuo, Data Reconnaissance and Injection (Ph.D. thesis), California State Polytechnic University, Pomona, CA, USA, 2017.
[65] T. Olavsrud, 11 Steps attackers took to crack target. 2014, 2014, https://www.cio.com/article/2600345/11-steps-attackers-took-to-crack-target.html. (Accessed 18 August 2023).
[66] A Kill Chain Analysis of the 2013 Target Data Breach, Committee on Commerce, Science and Transportation, 2014, https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883. (Accessed 21 August 2023).
[67] X. Chen, J. Shi, R. Xu, S.M. Yiu, B. Fang, F. Xu, PAITS: Detecting masquerader via short-lived interventional mouse dynamics, in: L. Batten, G. Li, W. Niu, M. Warren (Eds.), Proceedings of the Applications and Techniques in Information Security, ATIS 2014, Vol. 490, Springer, New York, NY, USA, 2014, pp. 231–242.
[68] E. Yuan, S. Malek, Mining software component interactions to detect security threats at the architectural level, in: Proceedings of the 13th Working IEEE/IFIP Conference on Software Architecture Mining, Venice, Italy, 2016, pp. 211–220.
[69] T. Zhang, P. Zhao, Insider threat identification system model based on rough set dimensionality reduction, in: Proceedings of the 2010 Second WRI World Congress on Software Engineering Insider, Vol. 2, IEEE, Boston, MA, USA, 2010, pp. 111–114.
[70] H. Lamba, T.J. Glazier, B. Schmerl, J. Camara, D. Garlan, J. Pfeffer, A model-based approach to anomaly detection in software architectures, in: Proceedings of the Symposium and Bootcamp on the Science of Security, Pittsburgh, PA, USA, 2016, pp. 69–71.
[71] S. Young, A. Dahnert, DevEyes insider threat detection, in: Proceedings of the 2011 Second Worldwide Cybersecurity Summit, WCS, IEEE, London, UK, 2011.
[72] L. Nkosi, P. Tarwireyi, M.O. Adigun, Insider threat detection model for the cloud, in: Proceedings of the 2013 Information Security for South Africa, Johannesburg, South Africa, 2013, pp. 1–8.
[73] Y. Park, I.M. Molloy, S.N. Chari, Z. Xu, C. Gates, N. Li, Learning from others: User anomaly detection using anomalous samples from other users, in: G. Pernul, P.Y.A. Ryan, E. Weippl (Eds.), Proceedings of the Computer Security-ESORICS 2015, PT II, Springer, New York, NY, USA, 2015, pp. 396–414.
[74] P. Parveen, N. McDaniel, Z. Weger, J. Evans, B. Thuraisingham, K. Hamlen, L. Khan, Evolving insider threat detection stream mining perspective, Int. J. Artif. Intell. Tools 22 (2013) 1360013.
[75] N. Pitropakis, C. Lambrinoudakis, D. Geneiatakis, Till all are one: Towards a unified cloud IDS, in: S. Fischer Hubner, C. Lambrinoudakis, J. Lopez (Eds.), Proceedings of the Trust, Privacy and Security in Digital Business, Springer, New York, NY, USA, 2015, pp. 136–149.
[76] J. Nikolai, Y. Wang, A system for detecting malicious insider data theft in IaaS cloud environments, in: Proceedings of the 2016 IEEE Global Communications Conference, GLOBECOM, Washington, DC, USA, 2016, pp. 1–6.
[77] S.C. Roberts, J.T. Holodnak, T. Nguyen, S. Yuditskaya, M. Milosavljevic, W.W. Streilein, A model-based approach to predicting the performance of insider threat detection systems, in: Proceedings of the 2016 IEEE Security and Privacy Workshops, SPW, Oxford, UK, 2016, pp. 314–323.
[78] W. Liu, L. Ci, L. Liu, Research on behavior trust based on Bayesian inference in trusted computing networks, in: Proceedings of the 2015 IEEE International Conference on Smart City/SocialCom/SustainCom, SmartCity, Chengdu, China, 2015, pp. 1134–1138.
[79] H.G. Goldberg, W.T. Young, A. Memory, T.E. Senator, Explaining and aggregating anomalies to detect insider threats, in: Proceedings of the 2016 49th Hawaii International Conference on System Sciences, HICSS, Kauai, HI, USA, 2016, pp. 2739–2748.
[80] S. Rajamanickam, S. Vollala, R. Amin, N. Ramasubramanian, Insider attack protection: Lightweight password-based authentication techniques using ECC, IEEE Syst. J. (2019) 1–12.
[81] C.V. Neu, A.F. Zorzo, A.M.S. Orozco, R.A. Michelin, An approach for detecting encrypted insider attacks on OpenFlow SDN Networks, in: Proceedings of the 2016 11th International Conference for Internet Technology and Secured Transactions, ICITST, Barcelona, Spain, 2016, pp. 210–215.
[82] Z. Yan, W. Ding, V. Niemi, A.V. Vasilakos, Two schemes of privacy-preserving trust evaluation, Futur. Gener. Comput. Syst. 62 (2016) 175–189.

[83] A. Zargar, A. Nowroozi, R. Jalili, XABA: A zero-knowledge anomaly-based behavioral analysis method to detect insider threats, in: Proceedings of the 2016 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology, ISCISC, Tehran, Iran, 2016, pp. 26–31.

[84] A. Ambre, N. Shekokar, Insider threat detection using log analysis and event correlation, in: Proceedings of the International Conference on Advanced Computing Technologies and Applications, ICACTA-2015, Vol. 45, Elsevier B.V., Amsterdam, The Netherlands, 2015, pp. 436–445.

[85] I. Rose, N. Felts, A. George, E. Miller, M. Planck, Something is better than everything: A distributed approach to audit log anomaly detection, in: Proceedings of the 2017 IEEE Cybersecurity Development, SecDev, Cambridge, MA, USA, 2017, pp. 77–82.

[86] Y. Hu, B. Panda, Two-dimensional traceability link rule mining for detection of insider attacks, in: Proceedings of the 2010 43rd Hawaii International Conference on System Sciences, Honolulu, HI, USA, 2010, pp. 1–9.

[87] G. Garkoti, S.K. Peddoju, R. Balasubramanian, Detection of insider attacks in cloud based e-healthcare environment, in: Proceedings of the 2014 International Conference on Information Technology, Zrenjanin, Serbia, 2014, pp. 195–200.

[88] J. Blasco, J.E. Tapiador, P. Peris-Lopez, G. Suarez-Tangil, Hindering data theft with encrypted data trees, J. Syst. Softw. 101 (2015) 147–158.

[89] C. Gates, N. Li, Z. Xu, S.N. Chari, I. Molloy, Y. Park, Detecting insider information theft using features from file access logs, in: M. Kutyłowski, J. Vaidya (Eds.), Proceedings of the Computer Security-Esorics 2014, PT II, Vol. 8713, Springer, Cham, Switzerland, 2014, pp. 383–400.

[90] S. Gupta, C. Hanson, C.A. Gunter, M. Frank, D. Liebovitz, B. Malin, Modeling and detecting anomalous topic access, in: Proceedings of the 2013 IEEE International Conference on Intelligence and Security Informatics, Seattle, WA, USA, 2013, pp. 100–105.

[91] E. Costante, J. den Hartog, M. Petkovi'c, S. Etalle, M. Pechenizkiy, A white-box anomaly-based framework for database leakage detection, J. Inf. Secur. Appl. 32 (2017) 27–46.

[92] P.A. Legg, O. Buckley, M. Goldsmith, S. Creese, Automated insider threat detection system using user and role-based profile assessment, IEEE Syst. J. 11 (2017) 503–512.

[93] S. Aditham, N. Ranganathan, S. Katkoori, Memory access pattern based insider threat detection in big data systems, in: Proceedings of the 2016 IEEE International Conference on Big Data, Big Data, IEEE, Washington, DC, USA, 2016, pp. 3625–3628.

[94] H. Jaenisch, J. Handley, Insider threat detection enabled by converting user applications into fractal fingerprints and autonomously detecting anomalies, in: Proceedings of the Proceedings of SPIE-The International Society for Optical Engineering, Brussels, Belgium, 2012, p. 8408.

[95] S.L. Garfinkel, N. Beebe, L. Liu, M. Maasberg, Detecting threatening insiders with lightweight media forensics, in: Proceedings of the 2013 IEEE International Conference on Technologies for Homeland Security, HST, Waltham, MA, USA, 2013, pp. 86–92.

[96] T. Nathezhtha, V. Yaidehi, Cloud insider attack detection using machine learning, in: Proceedings of the Proceedings of the 2018 International Conference on Recent Trends in Advanced Computing, ICRTAC-CPS 2018, IEEE, Chennai, India, 2018, pp. 60–65.

[97] H. Bao, R. Lu, B. Li, R. Deng, BLITHE: Behavior rule-based insider threat detection for smart grid, IEEE Internet Things J. 3 (2016) 190–205.

[98] A.S. Sohal, R. Sandhu, S.K. Sood, V. Chang, A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments, Comput. Secur. 74 (2018) 340–354.

[99] M.A. Mohammed, S.M. Kadhem, A.A. Maisa'a, Insider attacker detection using light gradient boosting machine, Tech-Knowl. 1 (1) (2021) 67–76.

[100] W. Jiang, Y. Tian, W. Liu, W. Liu, An insider threat detection method based on user behavior analysis, in: International Conference on Intelligent Information Processing, Springer, 2018, pp. 421–429.

[101] N. Garba, S. Rakshit, C.D. Mang, N.R. Vajjhala, An email content-based insider threat detection model using anomaly detection algorithms, in: Proceedings of the International Conference on Innovative Computing & Communication, 2021, pp. 1–5.

[102] A. Diop, N. Emad, T. Winter, M. Hilia, Design of an ensemble learning behavior anomaly detection framework, Int. J. Comput. Inf. Eng. 13 (10) (2019) 547–555.

[103] E. Pantelidis, G. Bendiab, S. Shiaeles, N. Kolokotronis, Insider threat detection using deep autoencoder and variational autoencoder neural networks, in: 2021 IEEE International Conf. on Cyber Security and Resilience, CSR, IEEE, 2021, pp. 129–134.

[104] P. Chattopadhyay, L. Wang, Y.P. Tan, Scenario-based insider threat detection from cyber activities, IEEE Trans. Comput. Soc. Syst. 5 (3) (2018) 660–675.

[105] D.C. Le, A.N. Zincir-Heywood, Evaluating insider threat detection workflow using supervised and unsupervised learning, in: 2018 IEEE Security and Privacy Workshops, SPW, IEEE, 2018, pp. 270–275.

[106] F. Yuan, Y. Cao, Y. Shang, Y. Liu, J. Tan, B. Fang, Insider threat detection with deep neural network, in: International Conference on Computational Science, Springer, 2018, pp. 43–54.

[107] Y.A. Suh, M.S. Yim, High risk non-initiating insider identification based on EEG analysis for enhancing nuclear security, Ann. Nucl. Energy 113 (2018) 308–318.

[108] P.J. Taylor, C.J. Dando, T.C. Ormerod, L.J. Ball, M.C. Jenkins, A. Sandham, T. Menacere, Detecting insider threats through language change, LAW Hum. Behav. 37 (2013) 267–275.

[109] B. Zou, M. Yang, J. Guo, J. Wang, E.R. Benjamin, H. Liu, W. Li, Insider threats of Physical Protection Systems in nuclear power plants: Prevention and evaluation, Prog. Nucl. Energy 104 (2018) 8–15.

[110] F.A. Duran, Probabilistic basis and assessment methodology for effectiveness of protecting nuclear materials, in: 2012 IEEE Int. Carnahan Conf. on Security Tech., ICCST, IEEE, 2012, pp. 43–52.

[111] L. Fridman, S. Weber, R. Greenstadt, M. Kam, Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location, IEEE Syst. J. 11 (2017) 513–521.

[112] K. Al tabash, J. Happa, Insider-threat detection using Gaussian mixture models and sensitivity profiles, Comput. Secur. 77 (2018) 838–859.

[113] X. Wang, Q. Tan, J. Shi, S. Su, M. Wang, Insider threat detection using characterizing user behavior, in: Proceedings of the 2018 IEEE 3rd International Conference on Data Science in Cyberspace, DSC 2018, Guangzho, China, 2018, pp. 476–482.

[114] C. Xiaojun, W. Zicheng, P. Yiguo, S. Jinqiao, A continuous re-authentication approach using ensemble learning, Procedia Comput. Sci. 17 (2013) 870–878.

[115] B. Gabrielson, Who really did it? Controlling malicious insiders by merging biometric behavior with detection and automated responses, in: Proceedings of the 45th Hawaii International Conference on System Sciences Who, Maui, HI, USA, 2012, pp. 2441–2449.

[116] P.M. Nasr, A. Yazdian-Varjani, Toward operator access management in SCADA system: Deontological threats mitigation, IEEE Trans. Ind. Inform. 14 (2017) 3314–3324.

[117] F.Y. Leu, K.L. Tsai, Y.T. Hsiao, C.T. Yang, An internal intrusion detection and protection system by using data mining and forensic techniques, IEEE Syst. J. 11 (2017) 427–438.

[118] J. Maestre Vidal, A. Lucila Sandoval Orozco, L. Javier García Villalba, Online masquerade detection resistant to mimicry, Expert Syst. Appl. 61 (2016) 162–180.

[119] J. Clark, S. Leblanc, S. Knight, Compromise through USB-based Hardware Trojan Horse device, Futur. Gener. Comput. Syst. 27 (2011) 555–563.

[120] C.J. Fung, D.Y. Lam, R. Boutaba, RevMatch: An efficient and robust decision model for collaborative malware detection, in: Proceedings of the 2014 IEEE Network Operations and Management Symposium, NOMS, Krakow, Poland, 2014, pp. 1–9.

[121] H. Bostani, M. Sheikhan, Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach, Comput. Commun. 98 (2017) 52–71.

[122] Y. Hori, T. Nishide, K. Sakurai, Towards countermeasure of insider threat in network security, in: Proceedings of the 2011 Third International Conference on Intelligent Networking and Collaborative Systems, Fukuoka, Japan, 2011, pp. 634–636.

[123] D.N. Muchene, K. Luli, C.A. Shue, Reporting insider threats via covert channels, in: Proceedings of the 2013 IEEE Security and Privacy Workshops Reporting, IEEE, San Francisco, CA, USA, 2013, pp. 68–71.

[124] J.L. Rrushi, NIC displays to thwart malware attacks mounted from within the OS, Comput. Secur. 61 (2016) 59–71.

[125] F. Callegati, S. Giallorenzo, A. Melis, M. Prandini, Cloud-of-things meets mobility-as-a-service: An insider threat perspective, Comput. Secur. 74 (2018) 277–295.

[126] J. Lopez, C. Alcaraz, R. Roman, Smart control of operational threats in control substations, Comput. Secur. 38 (2013) 14–27.

[127] W. Meng, X. Luo, W. Li, Y. Li, Design and evaluation of advanced collusion attacks on collaborative intrusion detection networks in practice, in: Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, 2016, pp. 1061–1068.

[128] Y. Chen, S. Nyemba, B. Malin, Detecting anomalous insiders in collaborative information systems, IEEE Trans. Dependable Secure Comput. 9 (2012) 332–344.

[129] A. Sallam, E. Bertino, Detection of temporal insider threats to relational databases, in: Proceedings of the 2017 IEEE 3rd International Conference on Collaboration and Internet Computing, CIC, San Jose, CA, USA, pp. 406–415.

[130] D.C. Le, N. Zincir-Heywood, Exploring anomalous behaviour detection and classification for insider threat identification, Int. J. Netw. Manag. 31 (4) (2021) e2109.

[131] O. Lo, W.J. Buchanan, P. Griffiths, R. Macfarlane, Distance measurement methods for improved insider threat detection, Secur. Commun. Netw. 2018 (2018) 5906368.

[132] A. Almehmadi, Micromovement behavior as an intention detection measurement for preventing insider threats, IEEE Access 6 (2018) 40626–40637.

[133] N.S. Safa, C. Maple, T. Watson, R. Von Solms, Motivation and opportunity based model to reduce information security insider threats in organisations, J. Inf. Secur. Appl. 40 (2018) 247–257.

[134] W. Park, Y. You, K. Lee, Detecting potential insider threat: Analyzing insiders' sentiment exposed in social media, Secur. Commun. Netw. 2018 (2018) 7243296.

[135] V. Mavroeidis, K. Vishi, A. Jøsang, A framework for data-driven physical security and insider threat detection, in: Proceedings of the International Conference on Advances in Social Networks Analysis and Mining, ASONAM, IEEE, Barcelona, Spain, 2018, pp. 1108–1115.

[136] S. Dietzel, J. Gürtler, F. Kargl, A resilient in-network aggregation mechanism for VANETs based on dissemination redundancy, Ad Hoc Netw. 37 (2016) 101–109.

[137] C. Soh, S. Yu, A. Narayanan, S. Duraisamy, L. Chen, Employee profiling via aspect-based sentiment and network for insider threats detection, Expert Syst. Appl. 135 (2019) 351–361.

[138] S. Eberz, K.B. Rasmussen, V. Lenders, I. Martinovic, Looks like Eve: exposing insider threats using eye movement biometrics, ACM Trans. Priv. Secur. 19 (1) (2016) 1–31.

[139] C. Brunner, A. Delorme, S. Makeig, Eeglab –an open source matlab toolbox for electrophysiological research, Biomed. Eng./Biomedizinische Techn. 58 (Suppl. 1) (2013).

[140] B.M. Babu, M.S. Bhanu, Prevention of insider attacks by integrating behavior analysis with risk based access control model to protect cloud, Procedia Comput. Sci. 54 (2015) 157–166.

[141] A. Tewari, P. Verma, An improved user identification based on keystroke-dynamics and transfer learning, Webology 19 (1) (2022) 5369–5387.

[142] P. Baynath, K.M. SunjivSoyjaudah, M. Heenaye-Mamode Khan, Machine learning algorithm on keystroke dynamics pattern, in: Presented at 2018 IEEE Conference on Systems, Process and Control, ICSPC, 2018, pp. 11–16.

[143] S. Krishnamoorthy, L. Rueda, S. Saad, H. Elmiligi, Identification of user behavioral biometrics for authentication using keystroke dynamics and machine learning, in: Proceedings of the 2018 2nd International Conference on Biometric Engineering and Applications, ICBEA '18, 2018.

[144] H.C. Chang, J. Li, C.S. Wu, M. Stamp, Machine learning and deep learning for fixed-text keystroke dynamics, in: Cybersecurity for Artificial Intelligence, Springer, Cham, 2022, pp. 309–329.

[145] L. Aversano, M. Bernardi, M. Cimitile, R. Pecori, Continuous authentication using deep neural networks ensemble on keystroke dynamics, PeerJ Comput. Sci. 7 (525) (2021) 1–27.

[146] Z. Chen, H. Cai, L. Jiang, W. Zou, W. Zhu, X. Fei, Keystroke dynamics based user authentication and its application in online examination, in: 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design, CSCWD, 2021, pp. 649–654.

[147] O. Verma Thapliyal, A. Kumar, Behavioral biometric based personal authentication in feature phones, Int. J. Elec. Comput. Engg. (IJECE) 12 (1) (2022) 802–815.

[148] I. Lamiche, G. Bin, Y. Jing, Z. Yu, A. Hadid, A continuous smartphone authentication method based on gait patterns and keystroke dynamics, J. Amb. Intell. Human. Comput. 10 (11) (2018) 4417–4430.

[149] A. Huang, S. Gao, J. Chen, L. Xu, A. Nathan, High security user authentication enabled by piezoelectric keystroke dynamics and machine learning, IEEE Sens. J. 20 (21) (2020) 13037–13046.

[150] A. Pentel, Predicting age and gender by keystroke dynamics and mouse patterns, in: 25th Conf. on User Modeling, Adaptation and Personalization, 2017, pp. 381–385.

[151] T. Murata, Petri nets: properties, analysis and applications, in: Proceedings of the IEEE, Vol. 77, (4) 1989, pp. 541–580.

[152] H. Ragavan, B. Panda, Mitigating malicious updates: prevention of insider threat to databases, in: Proceedings - 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2013, IEEE, 2013, pp. 781–788.

[153] H. Louise, M.A.E. Crockett, R.A. Elliot, The Zynq Book Tutorials for Zybo and ZedBoard, first ed., The Strathclyde Academic Media, Glasgow, 2015.

[154] M.R. Lehrfeld, Preventing the insider –blocking USB write capabilities to prevent IP theft, in: 2020 SoutheastCon, Vol. 2, 2020, pp. 1–7.

[155] S. Thombre, Freeware solution for preventing data leakage by insider for windows framework, in: 2020 International Conference on Computational Performance Evaluation, ComPE, 2020, pp. 44–47.

[156] F.M. Sibai, D.A. Menasce, Defeating the insider threat via autonomic network capabilities, in: 2011 Third Int. Conf. on Comm. Sys. and Netw, IEEE, 2011, pp. 1–10.

[157] M.C. Huebscher, J.A. McCann, A survey of autonomic computing–degrees, models, and applications, ACM Comput. Surv. 40 (2008) 1–28.

[158] N. Baracaldo, B. Palanisamy, J. Joshi, G-SIR: an insider attack resilient geo-social access control framework, IEEE Trans. Dependable Secure Comput. 16 (1) (2019) 84–98.

[159] M. Liu, M. Li, D. Sun, Z. Shi, B. Lv, P. Liu, Terminator, in: Proceedings of the 17th ACM International Conference on Computing Frontiers, ACM, New York, 2020, pp. 142–149.

[160] A.K. Jain, A. Ross, S. Pankanti, Biometrics: a tool for information security, IEEE Trans. Inf. Forensics Secur. 1 (2) (2006) 125–143.

[161] C. Barral, A. Tria, Fake fingers in fingerprint recognition: glycerin supersedes gelatin, in: V. Cortier, C. Kirchner, M. Okada, H. Sakurada (Eds.), Formal to Practical Security, in: Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2009, p. 5458.

[162] A. Almehmadi, K. El-Khatib, On the possibility of insider threat prevention using intent-based access control, IEEE Syst. J. 11 (2) (2017) 373–384.

[163] P. Maharjan, K. Shrestha, T. Bhatta, H. Cho, C. Park, M. Salauddin, M.T. Rahman, S.S. Rana, S. Lee, J.Y. Park, Keystroke dynamics based hybrid nanogenerators for biometric authentication and identification using artificial intelligence, Adv. Sci. 8 (15) (2021) 1–9.

[164] N. Sae-Bae, N. Memon, Distinguishability of keystroke dynamic template, PLoS One 17 (1) (2022) 1–10.

[165] C. Jadhav, S. Kulkami, S. Shelar, K. Shinde, N.V. Dharwadkar, Biometrie authentication using keystroke dynamics, in: 2017 International Conference on I-SMAC, IoT in Social, Mobile, Analytics and Cloud I-SMAC, 2017, pp. 870–875.

[166] C. Shi, J. Liu, H. Liu, Y. Chen, WiFi-enabled user authentication through deep learning in daily activities, ACM Trans. Internet Things 2 (2) (2021) 1–25.

[167] B. Bhana, S. Flowerday, Passphrase and keystroke dynamics authentication: Usable security, Comput. Secur. 96 (101925) (2020) 1–13.

[168] M. Chagarlamudi, B. Panda, Y. Hu, Insider threat in database systems: preventing malicious users' activities in databases, in: ITNG 2009-6th International Conference on Information Technology: New Generations, 2009.

[169] E. Erdin, H. Aksu, S. Uluagac, M. Vai, K. Akkaya, OS independent and hardwar-eassisted insider threat detection and prevention framework, in: Proceedings of the 2018 IEEE Military Communications Conference, MILCOM2018, IEEE, 2018, pp. 926–932.

[170] E. Costante, D. Fauri, S. Etalle, J. Den Hartog, N. Zannone, A hybrid framework for data loss prevention and detection, in: 2016 IEEE Security and Privacy Workshops, SPW, 2016, pp. 324–333.

[171] T. Al-Shehari, S. Zhioua, An empirical study of web browsers' resistance to traffic analysis and website fingerprinting attacks, Cluster Comput. 21 (4) (2018) 1917–1931.

[172] R.A. Alsowail, T. Al-Shehari, A multi-tiered framework for insider threat prevention, Electronics 10 (9) (2021) 1005.

[173] M. Raissi-Dehkordi, D. Carr, A multi-perspective approach to insider threat detection, in: Proceedings of the 2011-MILCOM 2011 Military Communications Conference, IEEE, Baltimore, MD, USA, 2011, pp. 1164–1169.

[174] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici, M. Ochoa, Insight into insiders: A survey of insider threat taxonomies, analysis, modeling, and countermeasures, ACM Comput. Surv. 52 (2019).

[175] S. Asha, D. Shanmugapriya, G. Padmavathi, Malicious insider threat detection using variation of sampling methods for anomaly detection in cloud environment, Comput. Electr. Eng. 105 (108519) (2023).

[176] L.S. Khorrami, A. Afshar, Attack detection in active queue management within large-scale networks control system with information of network and physical system, in: Proceedings of the 2016 24th Iranian Conference on Electrical Engineering, ICEE, Okinawa, Japan, 2016, pp. 714–719.

[177] D. Dasgupta, A. Roy, D. Ghosh, Multi-user permission strategy to access sensitive information, Inform. Sci. 423 (2018) 24–49.

[178] D. Zhou, K. Wang, N. Cao, J. He, Rare category detection on time-evolving graphs, in: Proceedings of the 2015 IEEE International Conference on Data Mining, Atlantic City, NJ, USA, 2015, pp. 1135–1140.

[179] K. Raghavan, M. Desai, P.V. Rajkumar, Multi-step operation strategic framework for ransomware protection, SAM Adv. Manag. J. 85 (4) (2020) 16-22.

[180] P.V. Rajkumar, R. Sandhu, Safety decidability for pre-authorization usage control with identifier attribute domains, IEEE Trans. Dependable Secure Comput. 17 (3) (2020) 465–478.

[181] P.V. Rajkumar, R. Sandhu, Safety decidability for pre-authorization usage control with finite attribute domains, IEEE Trans. Dependable Secure Comput. 13 (5) (2015) 582–590.

[182] P.V. Rajkumar, S.K. Ghosh, P. Dasgupta, Application specific usage control implementation verification, Int. J. Netw. Secur. Appl. 1 (3) (2009) 116–128.

[183] P.V. Rajkumar, S.K. Ghosh, P. Dasgupta, Concurrent usage control implementation verification using spin model checker, in: Recent Trends in Network Security and Applications, CNSA 2010, in: Communications in Computer and Information Science, vol. 89, Springer, 2010.

[184] P.V. Rajkumar, S.K. Ghosh, P. Dasgupta, An end to end correctness verification approach for application specific usage control, in: Proceedings of IEEE International Conference on Industrial and Information Systems, ICIIS, IEEE, Peradeniya, Sri Lanka, 2009, pp. 1–6.

[185] K. Viet, B. Panda, Y. Hu, Detecting collaborative insider attacks in information systems, in: Proceedings of the 2012 IEEE International Conference on Systems, Man, and Cybernetics, SMC, Seoul, Korea, 2012, pp. 502–507.

[186] S. Alneyadi, E. Sithirasenan, V. Muthukkumarasamy, A survey on data leakage prevention systems, J. Netw. Comput. Appl. 62 (2016) 137–152.

Ms. S. Asha is a Research Scholar at Avinashilingam Institute for Home Science and Higher Education for Women (Deemed to be University), Coimbatore, India. She was awarded as Vijayalakshmi Purushothaman (Master of Science in Information Technology). Her areas of interest include, Cyber Security and Biometric security. She is doing research under Centre for Cyber Intelligence, DST CURIE AI Phase II Project, Avinashilingam Institute for Home Science and Higher Education for Women. She has successfully completed In-House funded project sponsored by DST. She has 4 publications in prestigious conferences and 1 publication in peer-reviewed Elsevier journal, "Computers and Electrical Engineering".

Dr. D. Shanmugapriya is an Assistant Professor and Head, Department of Information Technology, Avinashilingam Institute for Home Science and Higher Education for Women (Deemed to be University), Coimbatore, India since 2001. She has more than 20 years of teaching experience and 10 years of research experience. Her areas of interest include, Cyber Security, Biometric security and Image Processing. She has executed funded projects sponsored by DRDO, DST and UGC. She is Supervising 3 scholars at Ph.D level. She has more than 25 publications in prestigious conferences and peer-reviewed journals. She is Reviewers for many Conferences and Journals. She is a content Writer of Virtual Currency, Block Chain Technology and Basics of Security Auditing for SWAYAM-MOOC course on Cyber Security.

Google Sites Profile Page: https://sites.google.com/avinuty.ac.in/drshanmugapriya.