IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Unified Classification Model to Prevent Insider Threats in Cloud Computing

P. Arul Selvam
Department of CSE
Hindusthan College of Engineering and Technology
Coimbatore
arulselvamme@gmail.com

ABSTRACT

In cloud computing public and private sectors are both spending a large portion of their budget to protect the confidentiality, integrity, and availability of their data from possible attacks. Among these attacks are insider attacks which are more serious than external attacks, as insiders are authorized users who have legitimate access to sensitive assets of an organization. As a result, several studies exist in the literature aimed to develop techniques and tools to detect and prevent various types of insider threats. A unified classification model is proposed to classify the insider threat prevention approaches into two categories biometric-based and asset-based metric. The biometric-based category is also classified into physiological, behavioral and physical, while the asset metricbased category is also classified into host, network and combined. This classification systematizes the reviewed approaches that are validated with empirical results and it shows significant theoretical and empirical factors that play a key role in the effectiveness of insider threat prevention approaches such as evaluation metrics.

Keywords: Cloud Computing, Security and privacy, Insider threat prevention, Evaluation Metrics

1. INTRODUCTION

Due to the spread use of technologies in the last decades, issues of security and privacy have been extremely increased. Organizations are holding sensitive assets (e.g., customer data, business plans, intellectual properties, etc.), which could cause a huge damage to their business and reputation, if they have been breached. Therefore, it is of great importance to all organizations to protect the confidentiality, integrity, and availability of their sensitive assets from insider attacks. One of the major concerns in the field of information security is the insider attacks [Ref. 1], as they were reported to be the most common attack in 2017 with around 60% [Ref. 2].

The insider threats are malicious acts that are carried out by authorized persons, which may cause detrimental implications for digital and physical assets of an organization. In [Ref. 3] an insider is defined as ‘‘any person who has some legitimate privileged access to internal digital resources, i.e., anyone who is allowed to see or change the organization’s computer settings, data, or programs in a way that arbitrary members of the public may not. The Computer and Emergency and Response Team (CERT) emphasized the malicious intention of the insider by defining the insider as ‘‘a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems'' [Ref. 4].

Whether malicious acts of insiders were intentional or unintentional, they can cause an equally harmful impact, such as stealing, leaking and damaging sensitive data, or even helping external attackers by creating backdoors for them to attack. The severity of attacks caused by insiders can be noticed from the following examples of occurred real-world incidents [Ref. 5]. The first example, a serious insider attack which destroyed the image of both the Federal Bureau of Investigation (FPI) and the U.S. was conducted by an employee of the U.S. National Security who leaked high confidential data to Russian agencies. Another insider attack was carried out by a soldier of the U.S. army who leaked huge highly classified government documents to WikiLeaks. Moreover, the most serious fraud incident, which cost the Societe Generale French bank an estimated amount of $7 billion, was conducted by one of its employees.

In addition, 1,154 actual insider threat incidents in [Ref. 6] were reported by the U.S. Security Service and CERT. Such insider attack incidents have been classified into different categories: sabotage, fraud, theft, and miscellaneous. A number of 659 from the reported incidents fell under the category of fraud in which data were modified or deleted for the aim of personal gain, whereas 189 of the reported incidents fell under the category of theft, where intellectual properties of organizations were stolen. The rest of the reported incidents fell under the categories of sabotage and miscellaneous, where the aim was to disrupt business operations of organizations. While some organizations have reported the occurred insider attack incidents, other organizations have not. This is because they are afraid of the negative impact that may face if the executed insider attack incidents are announced to the public [Ref. 7].

2. WORK FLOW

The reliance on the utilization of digital assets presents a real challenge on how to secure them. Such assets exist within the boundaries of the organizations in PCs, USB devices, emails, memo and networks. Securing such sensitive digital assets is of great importance to the continuity and advancement of organizations. To prevent insider threats, some companies have taken drastic measures, such as employee vetting, authentication mechanisms, training, surveillance, separation of duty, and so on [Ref. 8]. Insider threats are the most challenging to detect, and traditional techniques cannot easily mitigate them [Ref. 9].

CERT has contributed widely in such work by providing periodic guidelines that include the best practices for insider attack mitigation [Ref 10]. Different approaches for protecting against insider threats can be categorized into three classes (detection approaches, detection & prevention approaches, or prevention approaches). In the first class, insider threats are detected during or after the threat has happened. In the second class, insider threats are detected and then they are prevented but while or after some parts of the threats are happening. In the third class, insider threats are prevented before they are carried out. The third class is the optimal solution for insider threat prevention but the hardest to achieve. It is noticed that most of the existing approaches focused on the first class ''detection approaches''.

The huge damage caused by successful insider attacks to many organizations have made it crucial to prevent such attacks. In our research of interest, we conducted a thorough search to figure out the research gaps in the insider threat prevention area which are not addressed yet. Therefore, as different from existing surveys, our study reviews and discusses the insider threat prevention approaches by classifying them into major categories (biometrics, asset-metrics, etc.). Then, it discusses and compares them from different theoretical and empirical aspects. The proposed classification model, discussed empirical and conceptual factors, and highlighted research challenges will provide the insider threat research community with updated review for devising more effective insider threat prevention.

A unified classification model is proposed to classify the insider threat prevention approaches into two categories (biometric and asset-metric). The biometric-based category is also classified into (physiological, behavioral and physical), while the asset metric-based category is also classified into (host, network and combined). Such classification model systematizes the insider threat prevention approaches based on the major factors that play a key role in insider threat prevention contexts. It discusses some significant factors (theoretical and empirical) that affect the performance and the scope of insider threat prevention approaches.

3. IMPLEMENTATION

As mentioned above, tremendous losses have been incurred due to the rising number of insider attacks. As a result, various solution approaches have been introduced in the literature, most of them are focused on the detection approach ‘‘how to detect insider attacks’’ which have been reviewed in [Ref. 11-14]. In this section we demonstrate our classification model as depicted in Fig. 1.

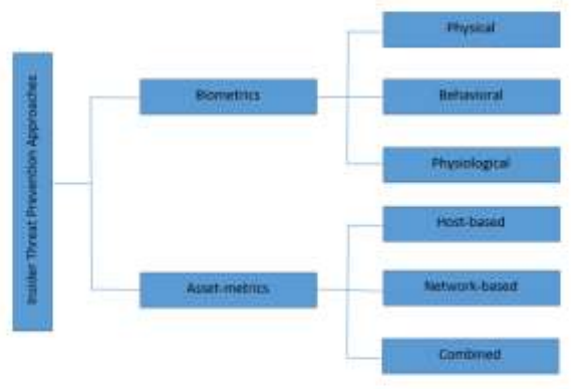

Fig. 1: Proposed classification model of the insider threat prevention approaches

3.1 Biometric-based

The reality is that insider threats are human-based, and hence should be dealt with by employing biometrics. Biometric technology is the analysis of a person’s physical, physiological or behavioral features [Ref. 15]. A number of approaches, illustrated in the subsequent sections, have been applied to validate legitimate users from fraudsters. Some strategies have made use of the brain signals, typing behaviors, eye movements, and body movements of insiders for the aim of preventing insider threats.

3.1.1 Physical biometrics

Applying human-based characteristics (biometric measurements) in the field of information security has been an active area of research for many years. It has continuously evolved from physical/hard biometrics (e.g., fingerprints, eye iris, and facial patterns) to physiological biometrics (e.g., brain signals). Physical biometrics enable the discrimination between individuals with high accuracy rate, which cannot usually be changed during the lifetime of a person [Ref. 16]. However, although physical biometrics is hard to be mimicked, it can still be exploited by attackers due to the high-level advancements in technology gadgets. For example, [Ref. 17] showed that fingerprint sensors can be attacked using mock fingers. In addition, [Ref. 18] presented that a facial recognition attack is possible using complex 3D video software. Thus, a research gap that can be bridged here to prevent this type of insider attacks. This can be achieved by developing a continuous authentication mechanism by utilizing physical biometrics (e.g., eye iris or facial patterns) to verify insiders throughout their sessions continuously.

3.1.2 Behavioral biometrics

Various biometrics have been used to improve the protection against insider attacks.

Behavioral biometric was introduced by some of the reviewed approaches (e.g., typing patterns, head and eye motions). One science of biometric is Keystroke dynamics, where insiders, based on their typing habit, are authenticated constantly. The Proposed approach which aims at detecting and preventing masqueraders' attacks by integrating typing patterns of insiders with an access control model. The model is made up of two phases. Risk scores are linked to resources using Common Vulnerability Scoring System (CVSS) in the first phase, and continuous validation of insider typing is tracked during the whole session (using keyloggers) in the second phase. The Support Vector Machine (SVM), as a classifier, and CERT insider threat database were both utilized to conduct the simulation testing. The variations between presses and releases of insider keystroke patterns were calculated. Once an anomalous typing pattern is detected, the tasks in execution will immediately be blocked, as considered a masquerader attack. The risks in the model are categorized into low, medium, high and critical, and results are presented for different scenarios.

3.1.3 Physiological biometrics

The main goal of access control models is to regulate access to digital assets through various authentication methods, e.g., passwords, tokens, fingerprints, etc., so that access can only be granted to authorized users with the right permissions. A major problem of access control models in general is that once a user has been granted access to a digital asset, the user will be trusted throughout the session. Hence, the user will be able to misuse the granted privileges without being detected. To overcome this problem, Intent-Based Access control Model (IBAC) was proposed. Unlike traditional access control models, IBAC verifies the integrity of insiders' intent rather than their identities. The idea of IBAC is that physiological features, such as brain signals, can be utilized to detect the honesty of intentions for preventing insider threats, since such threats are human-based.

3.2 Asset-based metrics

In this section, we present the asset-based approaches which are categorized into host, network and combined.

3.2.1 Host-Based

A freeware Data Leakage Prevention (DLP) system [Ref. 19] was proposed to protect sensitive data in small and medium scale organizations. Although there are several channels for exfiltrating data (e.g., E-mail, Bluetooth, etc.), the USB is the most well-known channel for data transfer. So, the proposed DLP system is designed for the windows platform to prevent the transferring of confidential files through USB ports. The system is designed to monitor the move and copy operations that are conducted from a PC to any USB devices continuously. This can be done based on security policies and criteria that can be set by system administrators. For the aim of introducing a novel data leakage prevention solution, the proposed system leverages kernel space modules and machine learning for checking the contents of transferred files and blocking file transfer actions in case of confidential files.

3.2.2 Network-Based

For preventing insider threats over the network, the authors in [Ref. 20] proposed the Autonomic Violation Prevention System (AVPS). It is an extension to their previous work in [Ref. 20] that was concerned with the scalability of their approach. In their proposed system, access to a network is limited and controlled via in-line components that monitor the act of an insider on a network. Then, the insider act is taken based on associated conditions with incidents of data leakage threats. This was accomplished by the use of Event-Condition-Action (ECA) autonomic policies [Ref. 21], which are widely used in security-centric systems. Several tests were carried out to evaluate the performance of their system across a variety of network applications (e.g., FTP, database, and Web servers). The tests were conducted on RedHat, Ubuntu Linux, and Fedora operating systems. Snort was used to process network traffic packets and extract attributes (e.g., IP, user, application type, request, response, etc.). The information gathered was analyzed and normalized before being compared to policies and rules. When a breach is detected, an action is taken to prevent malicious transfers. The efficiency was assessed using three metrics: throughput, CPU consumption, and transfer time, all of which had 95% confidence intervals.

3.2.3 Combined

Since insiders have permissions to use a variety of organization resources, various attributes can be utilized to prevent possible malicious acts. The widespread use of mobile devices and social media presents an opportunity to be incorporated into protection systems. Obtaining geo-context information of insiders related to their work environments can help to detect suspicious insiders and hence prevent associated threats. Moreover, granting or denying access to an organization asset can be determined through such information [Ref. 22]. For example, an insider who constantly stands in positions where he/she is not supposed to be in should be flagged as suspicious and denied from accessing high-value assets by an ideal security system. Concerning this, in [Ref. 23] a Resilient Access Control Framework (G-SIR) was proposed to detect the trustworthiness of insiders before granting them an access to specific assets.

In [Ref. 24], a hybrid framework for intellectual property theft detection and prevention was proposed. It integrates a prevention module with an anomaly detection module. The prevention module utilized a blacklist mechanism for preventing known insider attacks through applying two phases (the prevention phase and the blacklist management phase). In the prevention phase, an insider activity is matched against a blacklist, so if it is included within the blacklist, the insider's act will be blocked and all homologous activities will be blocked as well. Otherwise, it is passed to the detection module for verifying whether it matches the previously known normal act or not. This is used for updating the profile of the normal activities model utilizing an operator who is responsible for analyzing the raised alert. So, if the alert is recognized as a false positive, the normal activities profile is updated, otherwise, it is identified as a malicious act. The decision to append it to the blacklist was based on the analysis knowledge of the operator. The experimental results showed that the framework can reduce the efforts of the operator by preventing insider acts within a time of around 0.5 Ms. The framework can also reduce the spread of intellectual property leakages as well as and the damages that may cause.

A comprehensive framework for preventing insider threats was proposed, as it analyzes three types of insider threat countermeasures: measures taken before insiders enter a company, measures taken during their working time within an organization, and measures taken after they depart an organization. Such countermeasures included technological, psychological, behavioral, and cognitive measures that lasted from before an insider joined the company until after they left.

4 Evaluation Metrics

The clear demonstration of evaluation results for an insider threat prevention approach is highly significant. It provides assessment metrics to show the accuracy and performance of an approach and the significance of reported results. It has been observed that the reviewed approaches utilized various evaluation metrics, as summarized in Table 1. It is observed that the works in [Ref. 25-27] focused on assessing the performance of their approaches (e.g., frequency, throughput, average response time and CPU utilization) rather than their accuracy in preventing malicious acts of insiders.

Metrics	Description
FN	False Negative (FN) is the number of malicious acts that are not prevented by an approach [Ref. 25].
RAM	Risk Assessment Matrix (RAM) calculates the risk level for an asset with respect to malicious acts of an insider [Ref. 26].
EER	Equal Error Rate (EER) is the rate of an intersection between False Acceptance Rate (FAR) and False Rejection Rate (FRR) [Ref. 27].
Frequency and time	Determine the performance of the approach by calculating the frequency of validations and the time taken to address the threats [Ref. 28].
Transferring time	The average time of transferring data from PC to USB device while preventing USB malicious code injections [Ref. 29].
FP	False Positive (FP) is the number of legitimate activities of an insider that are counted as malicious ones [Ref. 30].
Performance Measures	Determine the performance of the approach in terms of throughput, average response time, and CPU utilization [Ref. 31].
Accuracy and Acceptance Rate	The accuracy rate of preventing malicious acts from insiders, and the acceptance rate of insiders for the measurements devices mounted on their heads [Ref. 32].
TP, FN, FP and TN	True Positive (TP) is the percentage of malicious acts prevented correctly. False Negative (FN) is the percentage of malicious acts that are not prevented. False Positive (FP) is the percentage of legitimate acts of an insider that are counted wrongly by an approach as malicious ones. True Negative (TN) is the percentage of legitimate acts that are classified correctly as legitimate [Ref. 33].

Table 1: The evaluation metrics of reviewed approaches

On the other hand, the other reviewed approaches focused on evaluating the accuracy for preventing insider malicious acts using different metrics. For example, the approaches in [Ref. 34-35] were evaluated utilizing the accuracy rate and risk assessment matrix, respectively. With regard to the evaluation metrics, we believe that the TP, FN, FP and TN metrics are the best ones to assess the extent of how an approach is accurate in preventing insider malicious acts. These metrics are also known as a confusion matrix, which utilize several approaches [Ref. 36-38]. Table 2 shows a brief overview of the confusion matrix. Accordingly, an efficient insider threat prevention approach should minimize (FN and FP) and maximize (TP and TN). Therefore, we recommend such metrics to be utilized for evaluating future insider threat prevention approaches.

Action/ Reaction	Prevented	Not Prevented
Malicious Act	True Positive (TP)	False Negative (FN)
Legitimate Act	False Positive (FP)	True Negative (TN)

Table 2: Confusion matrix (accuracy metrics) of the insider threat prevention approaches

5 CONCLUSION AND FUTURE WORK

Organizations are facing an increasing number of insider threats. As insiders have privileged access to the assets of an organization, preventing insider threats is a challenging problem. In this article, we reviewed the techniques and countermeasures that have been proposed to prevent insider attacks. Proposed classification model that categorizes the existing approaches into two main classes: biometric-based and asset-based. The biometric-based approaches are further classified into physiological, behavioral and physical, while the asset-based approaches are classified into host, network and combined. Such classification will provide a better understanding of the existing works, and highlight some gaps that need to be bridged to institute more holistic solutions. In the future work, we aim to propose a comprehensive framework for preventing insider threats in large scale organizations. Several state-of-the-art technologies (e.g., blockchain, IoT, cloud computing, machine and deep learning, etc.) will be integrated for the aim of devising an all-encompassing insider threat prevention framework.

REFERENCES

[1] Yaseen Q, Panda B. 2012. Insider threat mitigation: preventing unauthorized knowledge acquisition. International Journal of Information Security 11(4):269–280 DOI 10.1007/s10207-012-0165-6.

[2] Lee C, Iesiev A, Usher M, Harz D, McMillen D. 2020. IBM X-force threat intelligence Index. Available at https://www.ibm.com/security/data-breach/threat-intelligence (accessed on 7 February 2021).

[3] Sinclair S, Smith SW. 2008. Preventative directions for insider threat mitigation via access control. In: Insider attack and cyber security. Boston: Springer USA, 165–194.

[4] Claycomb WR, Nicoll A. 2012. Insider threats to cloud computing: directions for new research challenges. In: 2012 IEEE 36th annual computer software and applications conference. Piscataway: IEEE,387–394 DOI 0.1109/COMPSAC.2012.113.

[5] Hunker J, Probst C. 2011. Insiders and insider threats—an overview of definitions and mitigation techniques. Journal of Wireless Mobile Networks, Ubiquitous Computing Dependable Applications 2(1):4–27.

[6] Collins M. 2016. Common sense guide to mitigating insider threats. Pittsburgh: Carnegie-Melon, University of Pittsburgh.

[7] Roy Sarkar K. 2010. Assessing insider threats to information security using technical, behavioral and organizational measures. Information Security Technical Report 15(3):112–133 DOI 10.1016/j.istr.2010.11.002.

[8] Erdin E, Aksu H, Uluagac S, Vai M, Akkaya K. 2018. OS independent and hardwareassisted insider threat detection and prevention framework. In: Proceedings of the 2018 IEEE military communications conference (MILCOM2018). Piscataway: IEEE, 926–932 DOI 10.1109/MILCOM.2018.8599719.

[9] Almehmadi A. 2018. Micromovement behavior as an intention detection measurement for preventing insider threats. IEEE Access 6:40626–40637 DOI 10.1109/ACCESS.2018.2857450.

[10] Silowash G, Cappelli D, Moore A, Trzeciak R, Shimeall TJ, Flynn L. 2012. Common sense guide to mitigating insider threats 4th edition. Technical Report CMU/SEI2012-TR-012. Software Engineering Institute, Carnegie Mellon University, Pitts-burgh, Pennsylvania DOI 10.21236/ADA585500.

[11] Bertacchini M, Fierens PI. 2009. A survey on masquerader detection approaches. Available at http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia2- Sesion5(2).pdf .

[12] Ben Salem M, Hershkop S, Stolfo SJ. 2008. A survey of insider attack detection research. In: Insider attack and cyber Security. Boston: Springer USA, 69–90.

[13] Gheyas IA, Abdallah AE. 2016. Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. Big Data Analytics 1(1):6 DOI 10.1186/s41044-016-0006-0.

[14] Ko LL, Divakaran DM, Liau YS, V. Thing LL. 2017. Insider threat detection and its future directions. International Journal of Security and Networks 12(3):168–187 DOI 10.1504/IJSN.2017.084391.

[15] Jain AK, Ross A, Pankanti S. 2006. Biometrics: a tool for information security. IEEE Transactions on Information Forensics and Security 1(2):125–143 DOI 10.1109/TIFS.2006.873653.

[16] Eberz S, Rasmussen KB, Lenders V, Martinovic I. 2016. Looks like Eve: exposing insider threats using eye movement biometrics. ACM Transactions on Privacy and Security 19(1):1–31 DOI 10.1145/2904018.

[17] Barral C, Tria A. 2009. Fake fingers in fingerprint recognition: glycerin supersedes gelatin. In: Cortier V, Kirchner C, Okada M, Sakurada H, eds. Formal to practical security. Lecture notes in computer science, vol 5458. Berlin, Heidelberg: Springer DOI 10.1007/978-3-642-02002-5_4.

[18] Boehm A, Chen D, Frank M, Huang L, Kuo C, Lolic T, Martinovic I, Song D. 2014. SAFE: secure authentication with face and Eyes. In: 2013 international conference on privacy and security in mobile systems, PRISMS 2013 - co-located with global wireless summit. 1–8 DOI 10.1109/PRISMS.2013.6927175.

[19] Thombre S. 2020. Freeware solution for preventing data leakage by insider for windows framework. In: 2020 international conference on computational performance evaluation (ComPE). 044–047 DOI 10.1109/ComPE49325.2020.9200160.

[20] Sibai FM, Menascé DA. 2011. A scalable architecture for countering network-centric insider threats. In: SECURWARE 2011 - 5th international conference on emerging security information, systems and technologies, Nice/Saint Laurent du Var, France. 83–90.

[21] Huebscher MC, McCann JA. 2008. A survey of autonomic computing–degrees, models, and applications. ACM Computing Surveys 40:1–28 DOI 10.1145/1380584.1380585.

[22] Eberz S, Rasmussen KB, Lenders V, Martinovic I. 2016. Looks like Eve: exposing insider threats

using eye movement biometrics. ACM Transactions on Privacy and Security 19(1):1–31 DOI 10.1145/2904018.

[23] Baracaldo N, Palanisamy B, Joshi J. 2019. G-SIR: an insider attack resilient geo-social access control framework. IEEE Transactions on Dependable and Secure Computing 16(1):84–98 DOI 10.1109/TDSC.2017.2654438.

[24] Liu M, Li M, Sun D, Shi Z, Lv B, Liu P. 2020. Terminator. In: Proceedings of the 17th ACM international conference on computing frontiers. New York: ACM, 142–149 DOI 10.1145/3387902.3392329.

[25] Chagarlamudi M, Panda B, Hu Y. 2009. Insider threat in database systems: preventing malicious users' activities in databases. In: ITNG 2009 - 6th international conference on information technology: new generations.

[26] Almehmadi A, El-Khatib K. 2017. On the possibility of insider threat prevention using intent-based access control (IBAC). IEEE Systems Journal 11(2):373–384 DOI 10.1109/JSYST.2015.2424677.

[27] Eberz S, Rasmussen KB, Lenders V, Martinovic I. 2016. Looks like Eve: exposing insider threats using eye movement biometrics. ACM Transactions on Privacy and Security 19(1):1–31 DOI 10.1145/2904018.

[28] Ragavan H, Panda B. 2013. 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. Piscataway: IEEE, 781–788 DOI 10.1109/TrustCom.2013.95.

[29] Erdin E, Aksu H, Uluagac S, Vai M, Akkaya K. 2018. OS independent and hardware-assisted insider threat detection and prevention framework. In: Proceedings of the 2018 IEEE military communications conference (MILCOM2018). Piscataway: IEEE, 926–932 DOI 10.1109/MILCOM.2018.8599719.

[30] Costante E, Fauri D, Etalle S, Den Hartog J, Zannone N. 2016. A hybrid framework for data loss prevention and detection. In: 2016 IEEE security and privacy workshops (SPW). 324–333 DOI 10.1109/SPW.2016.24.

[31] Sibai FM, Menasce DA. 2011. Defeating the insider threat via autonomic network capabilities. In: 2011 third international conference on communication systems and networks (COMSNETS 2011), Bangalore, India. 1–10 DOI 10.1109/COMSNETS.2011.5716431.

[32] Almehmadi A. 2018. Micromovement behavior as an intention detection measurement for preventing insider threats. IEEE Access 6:40626–40637 DOI 10.1109/ACCESS.2018.2857450.

[33] O'Madadhain J, Fisher D, Smyth P, White S, Boey Y-B. 2005. Analysis and visualization of network data using JUNG. Journal of Statistical Software 10(2):1–35.

[34] Almehmadi A. 2018. Micromovement behavior as an intention detection measurement for preventing insider threats. IEEE Access 6:40626–40637 DOI 10.1109/ACCESS.2018.2857450.

[35] Almehmadi A, El-Khatib K. 2017. On the possibility of insider threat prevention using intent-based access control (IBAC). IEEE Systems Journal 11(2):373–384 DOI 10.1109/JSYST.2015.2424677.

[36] Chagarlamudi M, Panda B, Hu Y. 2009. Insider threat in database systems: preventing malicious users' activities in databases. In: ITNG 2009 - 6th international conference on information technology: new generations.

[37] Costante E, Fauri D, Etalle S, Den Hartog J, Zannone N. 2016. A hybrid framework for data loss prevention and detection. In: 2016 IEEE security and privacy workshops (SPW). 324–333 DOI 10.1109/SPW.2016.24.

[38] Baracaldo N, Palanisamy B, Joshi J. 2019. G-SIR: an insider attack resilient geo-social access control framework. IEEE Transactions on Dependable and Secure Computing 16(1):84–98 DOI 10.1109/TDSC.2017.2654438.