IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Unified Classification Model to Prevent Insider Threats in Cloud Computing

Mr.M.Priyadharshan, Mrs.R.Gayathri

Department of CSE

Assistant Professor

Hindusthan College of Engineering and Technology

ABSTRACT

In cloud computing public and private sectors are spending a large element in their price range to defend the confidentiality, integrity, and availability in their facts from possible attacks. Among those attacks are insider attacks that are greater critical than outdoors attacks, as insiders are certified clients who've respectable get proper of access to to sensitive property of an organization. As a result, limitless studies exist with inside the literature aimed to decorate techniques and system to take a look at and stop a number of sorts of insider threats. A unified type model is proposed to categorize the insider chance prevention approaches into lessons biometric-primarily based totally and asset-primarily based totally metric. The biometric-primarily based totally elegance is moreover categorized into physiological, behavioral and physical, even as the asset metric based elegance is moreover categorized into host, network and combined. This type systematizes the reviewed techniques which can be proven with empirical consequences and it shows widespread theoretical and empirical factors that play a key characteristic with inside the effectiveness of insider chance prevention approaches which includes contrast.

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

1. INTRODUCTION

Due to the unfold use of technology with inside the final decades, problems of safety and privateness had been extraordinarily increased. Organizations are protecting touchy belongings (e.g., patron data, commercial enterprise plans, highbrow properties, etc.), that may motive a massive harm to their commercial enterprise and reputation, in the event that they had been breached. Therefore, it's miles of fantastic significance to all companies to defend the confidentiality, integrity, and availability in their touchy belongings from insider attacks. One of the most important issues with inside the subject of records safety is the insider attacks [Ref. 1], as they had been pronounced to be the maximum not unusual place assault in 2017 with round 60% [Ref. 2].

The insider threats are malicious acts which might be finished through legal persons, which may also purpose unfavorable implications for virtual and bodily property of an organization. In [Ref. 3] an insider is described as ``any character who has a few valid privileged get admission to to inner virtual resources, i.e., all of us who's allowed to peer or extrude the organization`s pc settings, records, or packages in a manner that arbitrary participants of the general public may also not. The Computer and Emergency and Response Team (CERT) emphasized the malicious purpose of the insider with the aid of using defining the insider as ``a modern-day or former employee, contractor, or enterprise companion who has or had legal get admission to an organization`s network, system, or records and deliberately passed or misused that get admission to in a way that negatively affected the confidentiality, integrity, or availability of the organization`s facts or facts systems [Ref. 4].Whether malicious acts of insiders had been intentional or unintentional, they are able to purpose an similarly dangerous impact, which include stealing, leaking and detrimental touchy information, or maybe assisting outside attackers through developing backdoors for them to assault. The severity of assaults because of insiders may be observed from the subsequent examples of happened real-international incidents [Ref. 5]. The first example, a severe insider assault which destroyed the picture of each the Federal Bureau of Investigation (FPI) and the U.S. changed into carried out through a worker of the U.S. National Security who leaked excessive private information to Russian agencies. Another insider assault changed into executed through a soldier of the U.S. military who leaked big tremendously labelled authorities' files to WikiLeaks. Moreover, the maximum severe fraud incident, which fee the Society General French financial institution and predicted quantity of $7 billion, changed into carried out through certainly considered one among its employees.

In addition, 1,154 real insider risk incidents in [Ref. 6] have been stated with the aid of using the U.S. Security Service and CERT. Such insider assault incidents were categorized into extraordinary categories: sabotage, fraud, theft, and miscellaneous. A wide variety of 659 from the stated incidents fell beneath the class of fraud wherein information have been changed or deleted for the purpose of private gain, while 189 of the stated incidents fell beneath the class of theft, in which highbrow homes of businesses have been stolen. The relaxation of the stated incidents fell beneath the kinds of sabotage and miscellaneous, in which the purpose changed into to disrupt enterprise operations of businesses. While a few businesses have stated the happened insider assault incidents, different businesses have not. This is due to the fact they're scared of the bad effect which could face if the completed insider assault incidents are introduced to the public [Ref. 7].

2. WORK FLOW

The reliance at the usage of virtual property provides a actual mission on the way to steady them. Such property exist in the barriers of the businesses in PCs, USB devices, emails, memo and networks. Securing such touchy virtual property is of amazing significance to the continuity and development of businesses. To save you insider threats, a few organizations have taken drastic measures, which includes worker vetting, authentication mechanisms, training, surveillance, separation of duty, and so on [Ref. 8]. Insider threats are the maximum hard to detect, and conventional strategies cannot effortlessly mitigate them [Ref. 9].

CERT has contributed extensively in such paintings with the aid of using imparting periodic recommendations that encompass the first-class practices for insider assault mitigation [Ref 10]. Different processes for shielding towards insider threats may be labeled into 3 classes (detection processes, detection & prevention processes, or prevention processes). In the primary elegance, insider threats are detected in the course of or after the hazard has happened. In the second one elegance, insider threats are detected after which they're avoided however even as or after a few components of the threats are happening. In the 0.33 elegance, insider threats are avoided earlier than they're carried out. The 0.33 elegance is the highest quality answer for insider hazard prevention however the toughest to achieve. It is observed that maximum of the present processes centered on the primary elegance "detection processes". The large harm because of a hit insider assaults to many groups have made it critical to save you such assaults. In our studies of interest, we carried out a radical seek to parent out the studies gaps with inside the insider chance prevention place which aren't addressed yet. Therefore, as one of a kind from present surveys, our examine critiques and discusses the insider chance prevention procedures through classifying them into main categories (biometrics, asset-metrics, etc.). Then, it discusses and compares them from one of a kind theoretical and empirical aspects. The proposed type model, mentioned empirical and conceptual factors, and highlighted studies demanding situations will offer the insider chance studies network with up to date evaluate for devising extra powerful insider chance prevention.

A unified category version is proposed to categorize the insider chance prevention techniques into categories (biometric and asset-metric). The biometric-primarily based totally class is likewise categorized into (physiological, behavioral and physical), even as the asset metric-primarily based totally class is likewise categorized into (host, community and combined). Such category version systematizes the insider chance prevention techniques primarily based totally at the important elements that play a key position in insider chance prevention contexts. It discusses a few huge elements (theoretical and empirical) that have an effect on the overall performance and the scope of insider chance prevention techniques.

3. IMPLEMENTATION

As cited above, excellent losses had been incurred because of the growing range of insider attacks. As a result, diverse answer tactics had been delivered within side the literature, maximum of them are targeted at the detection approach ``the way to discover insider attacks`` that have been reviewed in [Ref. 11-14]. In this phase we show our category version as depicted in Fig. 1.

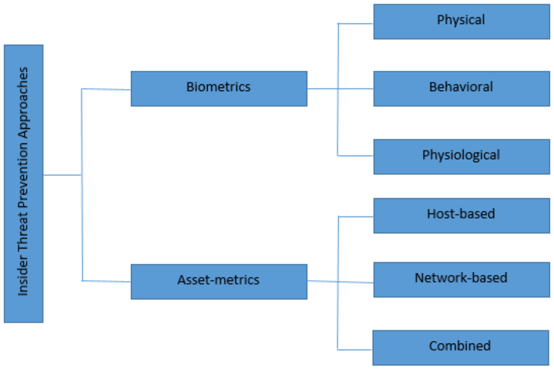

Fig. 1: Proposed classification model of the insider threat prevention approaches

3.1Biometric-based

The truth is that insider threats are human-based, and as a result ought to be handled via way of means of using biometrics. Biometric era is the evaluation of a person`s physical, physiological or behavioral features [Ref. 15]. A variety of approaches, illustrated within side the next sections, were implemented to validate valid customers from fraudsters. Some techniques have made use of the mind signals, typing behaviors, eye moves, and frame moves of insiders for the intention of stopping insider threats.

3.1.1 Physical biometrics

Applying human-primarily based totally characteristics (biometric measurements) with inside the subject of records safety has been an energetic place of studies for lots years. It has constantly developed from physical/difficult biometrics (e.g., fingerprints, eye iris, and facial patterns) to physiological biometrics (e.g., mind signals). Physical biometrics allow the discrimination among people with excessive accuracy rate, which can not normally be modified in the course of the life of a person [Ref. 16]. However, even though bodily biometrics is difficult to be mimicked, it is able to nonetheless be exploited with the aid of using Attackers because of the high-stage improvements in generation gadgets. For example, [Ref. 17] confirmed that fingerprint sensors may be attacked the usage of mock fingers. In addition, [Ref. 18] supplied that a facial popularity assault is feasible the usage of complicated 3-D video software. Thus, a studies hole that may be bridged right here to save you this sort of insider attacks. This may be executed through growing a non-stop authentication mechanism through making use of bodily biometrics (e.g., eye iris or facial patterns) to affirm insiders at some stage in their periods continuously.

3.1.2 Behavioral biometrics

Various biometrics **had been** used **to** enhance the safety towards insider assaults. Behavioural biometric changed into delivered through a number of the reviewed approaches (e.g., typing styles, head and eye motions). One technology of biometric is Keystroke dynamics, in which insiders, primarily based totally on their typing habit, are authenticated constantly. The Proposed method which objectives at detecting and stopping masquerades' assaults through integrating typing styles of insiders with an get entry to manage version. The version is made from phases. Risk rankings are connected to assets the use of Common Vulnerability Scoring System (CVSS) with inside the first phase, and non-stop validation of insider typing is tracked for the duration of the entire session (the use of key loggers) with inside the 2nd phase. The Support Vector Machine (SVM), as a classifier, and CERT insider hazard database have been each applied to behaviour the simulation testing. The versions among presses and releases of insider keystroke styles have been calculated. Once an anomalous typing sample is detected, the responsibilities in execution will right away be blocked, as taken into consideration a masquerade attack. The dangers with inside the version are labelled into low, medium, excessive and critical, and effects are offered for exceptional scenarios.

3.1.3 Physiological biometrics

The important aim of get entry to manage fashions is to adjust get entry to to virtual belongings thru numerous authentication methods, e.g., passwords, tokens, fingerprints, etc., in order that get entry to can handiest be granted to legal customers with the proper permissions. A essential trouble of get entry to manage fashions in popular is that after a consumer has been granted get entry to to a virtual asset, the consumer can be relied on at some stage in the session. Hence, the consumer can be capable of misuse the granted privileges without being detected. To triumph over this trouble, Intent-Based Access manage Model (IBAC) turned into proposed. Unlike conventional get entry to manage fashions, IBAC verifies the integrity of insiders` motive in preference to their identities. The concept of IBAC is that physiological features, along with mind signals, may be applied to come across the honesty of intentions for stopping insider threats, for the reason that such threats are human-based Asset-based metrics

In this section, we gift the asset-primarily based totally techniques which can be classified into host, community and combined.

3.2.1 Host-Based

A freeware Data Leakage Prevention (DLP) device [Ref. 19] turned into proposed to defend touchy records in small and medium scale organizations. Although there are numerous channels for exfiltrating records (e.g., E-mail, Bluetooth, etc.), the USB is the maximum famous channel for records switch. So, the proposed DLP device is designed for the home windows platform to save you the shifting of personal documents via USB ports. The device is designed to display the flow and duplicate operations which might be performed from a PC to any USB gadgets continuously. This may be achieved primarily based totally on safety rules and standards that may be set through device administrators. For the goal of introducing a unique records leakage prevention solution, the proposed device leverages kernel area modules and system studying for checking the contents of transferred documents and blockading document switch moves in case of personal documents.

Network-Based

For stopping insider threats over the community, the authors in [Ref. 20] proposed the Autonomic Violation Prevention System (AVPS). It is an extension to their preceding paintings in [Ref. 20] that changed into involved with the scalability in their approach. In their proposed system, get admission to to a community is restricted and managed through in-line additives that display the act of an insider on a community. Then, the insider act is taken primarily based totally on related situations with incidents of records leakage threats. This changed into achieved through the usage of Event-Condition-Action (ECA) autonomic policies [Ref. 21], which might be broadly utilized in security-centric systems. Several checks have been accomplished to assess the overall performance in their device throughout a number of community applications (e.g., FTP, database, and Web servers). The checks have been performed on Red Hat, Ubuntu Linux, and Fedora working systems. Snort became used to technique community site visitors packets and extract attributes (e.g., IP, user, utility type, request, response, etc.). The statistics accumulated became analyzed and normalized earlier than being as compared to rules and rules. When a breach is detected, a motion is taken to save you malicious transfers. The performance became assessed the use of 3 metrics: throughput, CPU consumption, and switch time, all of which had 95% self-belief intervals.

3.2.2 Combined

Since insiders have permissions to apply quite a few employer resources, diverse attributes may be applied to save you feasible malicious acts. The vast use of cellular gadgets and social media affords a possibility to be integrated into safety systems. Obtaining geo-context facts of insiders associated with their paintings environments can assist to hit upon suspicious insiders and consequently save you related threats. Moreover, granting or denying get entry to to an employer asset may be decided thru such facts [Ref. 22]. For example, an insider who continuously stands in positions in which he/she isn't always imagined to be in have to be flagged as suspicious and denied from getting access to high-fee belongings through a perfect protection system. Concerning this, in [Ref. 23] a Resilient Access Control Framework (G-SIR) turned into proposed to discover the trustworthiness of insiders earlier than granting them an get right of entry to particular assets

In [Ref. 24], a hybrid framework for highbrow assets robbery detection and prevention changed into proposed. It integrates a prevention module with an anomaly detection module. The prevention module applied a blacklist mechanism for stopping regarded insider assaults via making use of phases (the prevention segment and the blacklist control segment). In the prevention segment, an insider pastime is matched towards a blacklist, so if it's far covered inside the blacklist, the insider`s act may be blocked and all homologous sports may be blocked as well. Otherwise, it's far exceeded to the detection module for verifying whether or not it fits the formerly regarded regular act or not. This is used for updating the profile of the regular sports version making use of an operator who's liable for reading the raised alert. So, if the alert is identified as a fake positive, the regular sports profile is updated, otherwise, it's far recognized as a malicious act. The choice to append it to the blacklist changed into primarily based totally at the evaluation expertise of the operator. The experimental consequences confirmed that the framework can lessen the efforts of the operator with the aid of using stopping insider acts inside a time of round 0.five Ms. The framework also can lessen the unfold of highbrow assets leakages in.

A complete framework for stopping insider threats became proposed, because it analyzes 3 styles of insider danger countermeasures: measures taken earlier than insiders input an organization, measures taken at some point of their operating time inside an organization, and measures taken when they leave an organization. Such countermeasures blanketed technological, psychological, behavioral, and cognitive measures that lasted from earlier than an insider joined the organization till when they left.

4 Evaluation Metrics

The clean demonstration of assessment consequences for an insider chance prevention technique is noticeably significant. It affords evaluation metrics to reveal the accuracy and overall performance of a technique and the importance of mentioned consequences. It has been discovered that the reviewed techniques applied diverse assessment metrics, as summarized in Table 1. It is discovered that the works in [Ref. 25-27] centered on assessing the overall performance in their approaches (e.g., frequency, throughput, and common reaction time and CPU utilization) as opposed to their accuracy in stopping 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 opposite hand, the opposite reviewed processes targeted on comparing the accuracy for stopping insider malicious acts the use of special metrics. For example, the processes in [Ref. 34-35] had been evaluated utilizing the accuracy price and hazard evaluation matrix, respectively. With regard to the assessment metrics, we trust that the TP, FN, FP and TN metrics are the fine ones to evaluate the volume of ways an method is correct in stopping insider malicious acts. These metrics also are called a confusion matrix, which make use of numerous processes [Ref. 36-38]. Table 2 suggests a short review of the confusion matrix. Accordingly, an green insider risk prevention method need to minimize (FN and FP) and maximize (TP and TN). Therefore, we advocate such metrics to be applied for comparing destiny insider risk prevention processes.

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 dealing with increasingly more insider threats. As insiders have privileged get right of entry to to the property of an organization, stopping insider threats is a hard problem. In this article, we reviewed the strategies and countermeasures which have been proposed to save you insider attacks. Proposed category version that categorizes the prevailing procedures into predominant classes: biometric-primarily based totally and asset-primarily based totally. The biometric-primarily based totally procedures are in addition categorized into physiological, behavioral and physical, at the same time as the asset-primarily based totally procedures are categorized into host, community and combined. Such category will offer a higher information of the prevailing works, and spotlight a few gaps that want to be bridged to institute extra holistic solutions. In the destiny work, we goal to recommend a complete framework for stopping insider threats in huge scale organizations. Several today's technologies (e.g., block chain, IoT, cloud computing, gadget and deep learning, etc.) might be incorporated for the goal of devising an all

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.