*Journal of Discrete Mathematical Sciences & Cryptography*
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 3, pp. 707–718
DOI : 10.47974/JDMSC-1743

# Analysis and detection of insider attacks using behaviour rule based architecture in enterprise multitenancy

Santosh Kumar Henge [#]
Aditya Upadhyay [†]
*Department of Directorate of Online Education*
*Manipal University Jaipur*
*Jaipur 302034*
*Rajasthan*
*India*

Ashok Kumar Saini [§]
*Department of Computer Science & Engineering*
*Manipal University Jaipur*
*Jaipur 302034*
*Rajasthan*
*India*

Neha Mishra [‡]
Dimpal Sharma[@]
Gajanand Sharma *
*Department of Computer Science & Engineering, Jaipur*
*JECRC University*
*Jaipur 303905*
*Rajasthan*
*India*

**Abstract**

The enterprise level data security and privacy are one of the focal key challenges to the pr enterprise and security companies to prevent private data from outside and inside attacks. The insider threats and attacks can pretense a real defense risk to the various internal

[#] *E-mail:* hingesanthosh@gmail.com, santosh.henge@jaipur.manipal.edu
[†] *E-mail:* adityaupadhyay144@gmail.com
[§] *E-mail:* shksaini@gmail.com
[‡] *E-mail:* neha.rbt@gmail.com
[@] *E-mail:* dimpal286@gmail.com
* *E-mail:* gajanan.sharma@gmail.com (Corresponding Author)

© Taru Publications

multi-tenants of various enterprises and companies. The data thievery by insiders of the companies is as a great deal the consequence of enterprises failing to execute the scheme and expertise to member of staff supervise activities and administrate the authenticated data-access to data as it the authentic spiteful activities of member of staff looking for economic benefits in multi-tenancy environment. This research composed with three major objectives: Description of insider attack causes with their impact factors; Implications of behavior rule-based architecture in enterprise multitenancy; Integration of behavior rules with prevention thresholds to control user accessibility for prevention of insider attacks and threats; This paper has described the efficient security scenario to avoid insider attaching complexities. This research is more helping the cyber security experts and network administrators to reduce the insider attacks by building the efficient monitoring intelligent system. The experimental scenarios built with125 authenticated, 29 non-authenticated internal users, and 62 authenticated, 18 non-authenticated external users of single enterprise level and avoided insider attacks and threats.

***Subject Classification:*** *Primary 68M25, Secondary 68P25, 68P27.*

***Keywords:*** *Enterprise multitenancy (EMT), Multi tenancy (MT), Cloud environment (CE), Insider threat (IT), Assessment-based management (AbM), Insider attacks (IA), Negotiation performers (NP), Careless performers (CP), Data access control (DAC), Spiteful insider performers (SIP), Technology knowledge performers (TKP).*

## 1. Introduction

The cloud computing (CC) is performing a key role in the assessment of professional life of mankind with effective accomplishment of various CC services such as application, software, storage, networking along with platform assets on a utility-based-pay basis. CC data security is continually the highest priority of CC service providers. The cyber-attacks on CC data confirm that there is a demand for uninterrupted research for discovering various revised ways to protect the CC data from unauthorized users such Insider Attacks (IAs) and Outside Attacks (OAs). The hazard that insiders pose to society, enterprises, business-trading and governmental and non- governmental organizations persist to be of grave anxiety [3]. Insider Threat (IT) has grown to be an extensively recognized problem and one of the major challenges in network and cybersecurity. This trend implies that threats require special detection methods, tools, and systems which involve the capability to enable precise and quick revealing of a mischievous insider. Numerous analyses of detection IT and, associated areas in dealing with IT and Insider Attack (IA) based issues have been intended.

The insider threats and attacks can pretense a real defense risk to the various internal multi-tenants of various enterprises and companies. In

present days, the latest business investigations, academic literatures, and surveys presented the unambiguous proofs to sustain the consequences of this ITs and its pervasiveness [3]. It has happened by gathering the basic and confidential information – by abuse the secure credentials [1]. In the year of 2014, the Verizon data breach Investigation Reports assured that the privilege violence was the largely frequent sort of IT and insider attack (IA) by so far [1]. The IT and IA is always implicated, and it can pretense a real protection risks to the enterprises and companies. The CA and CI will be sourced by unknown persons whose are deliberately malevolent, and it can be incredible as simple as someone breach an attachment loaded with malware which always permits or provide the chances to the outsiders to steal the private data and information [1]. The data thievery by insiders of the companies is as a great deal the consequence of enterprises failing to execute the scheme and expertise to member of staff supervise activities and administrate the authenticated data-access to data as it the authentic spiteful activities of member of staff looking for economic benefits in multi-tenancy environment. This research composed with three major objectives:

- Description of insider attack causes with their impact factors.
- Implications of behaviour rule-based architecture in enterprise multitenancy
- Integration of behaviour rules with prevention thresholds to control user accessibility for prevention of insider attacks and threats.

This paper has described the efficient security scenario to avoid or reduce the insider attaching complexities. This research is more helping the cyber security experts and network administrators to reduce the insider attacks by building the efficient monitoring intelligent system.

## 2. Related Work

Insider attacks are more complicated to identify comparatively outsiders attack due to gained allowable accessibility and access control. Researchers are proposed various techniques, methods, and models to detect and analyze the insiders' attacks and treats in EMT. Several analyses intended to expand the theoretical ability of ITs and IAs. But there are many constraints, such as a lack of real cases, biases in conclusions of decision making, which are a main concern and persist undistinguishable

[12]. This section has articulated the various existing methodologies and models with their methodology flow, statistical aspects, theoretical-technical feasibilities, and Its advantages and lagging issues.

Author J. Lee et. al. proposed the approach of Digital Twin of an IT Detection (ITD) Enterprise using Model-Based Systems Engineering. It created to deal with analysis and valuation constraints which ITD enterprises face expected to a need of ground truth and lost data. It experimented the test cases through Cameo enterprise architecture simulation toolkit. It has integrated with assortment of statistical-data, data-processing stages, data-analysis, and machine learning (ML) methods to assess and predict the implementation of the enterprises [4]. Author B. Bowen et. al. proposed Host and Network Sensors based design to Mitigate IT. The IA assaults by end-users with confidential intelligence about a system-are a increasing challenge for many companies. It has created an architecture for IT revealing which blends complementary monitoring array of values and auditing procedures [5].

Author P. Dhiman et. al. proposed Blockchain merkle-tree ethereum approach in enterprise MT cloud environment (CE). It highlights on using CE-MT with Blockchain (BC) to increase security and privacy in CE[6]. The same author has proposed another approach Implications of Secure Token Key in an EMT CMT using Brakersky–Gentry–Vaikuntanathan (BGV) Hybrid Homomorphic Encryption and it processed through multi-factor authentication–authorization modes. It stated that tested with 152 end-users by integrating six multi-tenants, five head tenants, and two enterprise levels [7]. The author Alaa proposed combating ITs to Enterprise [8]. The IT to the main system of company coming from workforce classified as an IT which threats very serious caution, and each enterprise wants to pay attention to ITs because the workforce and former employees and other business associates like contractors might have access to the enterprise computer system or know the firewalls to avoid harming the security system of the organization. This might lead to sabotaging of the information system (IS) or mismanagement of the data that an enterprise holds [8][10]. An insider tries to sabotage the system, they generally know the data in-out weak points of the system to start with, due to this the system will be vulnerable. As not only the number of international companies has grown but also the proportion of huge organizations which presently totally depend on ISs for efficiently operating their procedures, a threat to these ISs can be deemed as a direct threat to the operations of these companies [9][10].

The author Al-Mhiqani et.al. MN presented a taxonomy of contemporary insider types, motivation, access, level, IA profiling, property of consequence security, and methods implicated by IA to conduct attacks and it described the various IA and IT detection methodologies and evaluation metrics [12-26]. Author P. Dhiman proposed qualified scrutiny complications in cloud security along with Non-Homomorphic and Homomorphic Encryption Practices[27]. The same author has proposed study of Blockchain based secure models and advances based on different CMT services[28]. The author ArnauErola et.al. proposed detection of IT with deployment of CITD tool in 3- multinational organizations. This approach justified its implementation based on CITD tool and results achieved from employing the recognition system in real network infrastructure over a period of six months [29]. Author Legg, P. A et.al. proposed robotic IT detection system applying user and role-based profile evaluations which able of identifying IT within company[30].

IT is a continual concern for companies and corporates similarly that has fascinated the attention of the research community, resulting in numerous behavioral models and tools to tackle it. Researchers are projected various efficient security models and methods to detect, analyze and restrict the ITs and IAs. Most of researchers are tuned their models with access control rules and dictionary-based parameters. However, there is less level integration of multi-access control-based rule tuning and multi-level authentication techniques are missing in existing research. This research has addressed few IAs and ITs issues and integrated multi-access control-based rule tuning and multi-level authentication techniques.

## 3. Methodology

It is significant to recognize that there are numerous diverse categories of IT and IA performers. Each type of category is representing the important challenges to the enterprisers and organizations. The security of data is not guaranteed as there is always a risk of leakage of users' data. Rule based data access control can be used in a MT-CE to improve the security of data, as it is a decentralized approach [6][7]. Data is saved in unaffected form. The Rule based data access control encryption process and algorithmic sequences are needed to implicate hashing techniques which permitting calculations on encoded data without the need for decryption.

### 3.1 *Integration of Enterprise Multitenancy (EMT) Key-Parameters*

#### 3.1.1 Negotiation Performers (NP)

The NP based insiders with accessible secure credentials and computing strategies which are negotiation by outsiders with their back-door patches considered it as threat performers. The NP based insiders are more difficult to tackle because the genuine assaults are imminent from external cloud, pretension a great transaction inferior danger of being acknowledged.

#### 3.1.2 Careless Performers (CP)

The CP based insiders who interpretation the data accidentally like as member of staff who right to use company data through public Wi-Fi without the knowledge that it is unsecured. A huge numeral of data violation occurrences consequence from member of staff carelessness in the direction of data-protection processes, rules, and exercises.

#### 3.1.3 Spiteful Insider Performers (SIP)

The SIP insiders whose are destroy the EMT networks and hack the data deliberately. The SIP attacks performed by the former member of staff whose are install or execute the malware implicated applications in EMT networks and PC's.

#### 3.1.4 Technology Knowledge Performers (TKP)

The TKP Insiders whose react to secure challenges.

- The SIP insider attackers will use their knowledge of flaws and data-vulnerabilities to violate authorization and access responsive data and information.
- The SIP insider attackers can pretence the most hazardous insider threats which are probable to trade the secret information to exterior black-market bidders and parties.

The data thievery by insiders is as a great deal the result of EMT weakening to execute schemes, approaches, and expertise to scrutinize the member of staff behavior and manage the data access to as it the genuine spiteful behavior of a member of staff looking for economic achievement.

### 3.2 *Prevention of Insider Attacks and Threats*

To protect against the IA and IT, the EMT network departments will require to following the various efficient secure advances and methodologies to secure the EMT level networks and private. The IA and IT will create hug data loss to the companies, and it will damage entire secure networks. The EMTsecure networks are compromised easily by implication of IA and IT based malware application and back-door data-leakage scenarios. The worst-case scenario is the IT and IA based hackers will create the huge violation inside the internal network systems, regardless of all the awareness that enormous hacks like the present EMT facing the insider attacking problems. In the EMTlevel, the data can breach if any one of the employees misplaced or stolen his personal or office laptops or smart phones. The confidential information is sheltered no matter anywhere it ends up when it encrypts at the file-level. The EMTnetwork department administrators require secure tools and layers which enabling the proactive security layers with auto control and decision-making environment as shown in the Figure 1. In this paper, the IA and IT based challenges are addressed and put self-assured a grounded outline for understanding along with reflection on the attacks and threats which are insiders' pretence.

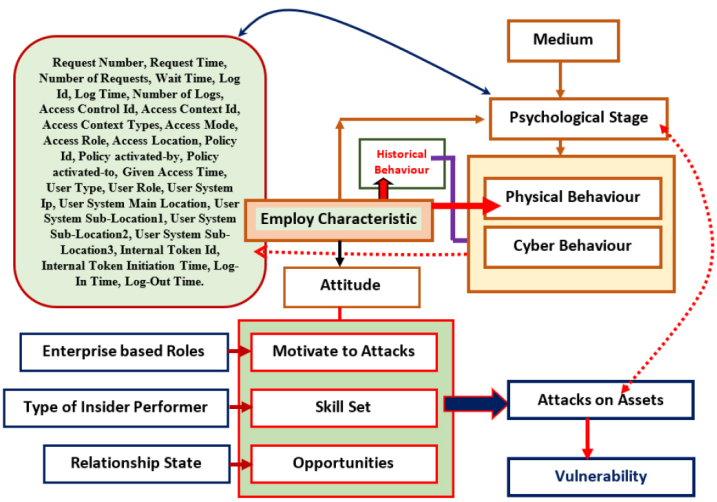


**Figure 1**

**Integration of multi-access control-based rule tuning and multi-level authentication techniques: IA and IT Attackers and Prevention Scenario**

The paper has implicated with the intelligence security systems (ISS) for avoiding the IA and IT security scenarios. The intelligence security systems (ISS) can be proficient to assessment, track control and manage the security issues and it enhanced with the security layers for protecting the data along with the workforce smart mobiles and personal PC's and laptops. The enhanced ISS has implicated with the settings of real-time on-demand security permission. In IIS, the EMTnetwork department administrators have addressed the ongoing IA and IT based security scenarios from stolen and misplaced devices. The implicated factors in proposed architecture as follow: Request Number, Request Time, Number of Requests, Wait Time, Log Id, Log Time, Number of Logs, Access Control Id, Access Context Id, Access Context Types, Access Mode, Access Role, Access Location, Policy Id, Policy activated-by, Policy activated-to, Given Access Time, User Type, User Role, User System Ip, User System Main Location, User System Sub-Location1, User System Sub-Location2, User System Sub-Location3, Internal Token Id, Internal Token Initiation Time, Log-In Time, Log-Out Time.The ISS based outline has categorize and recognize the numerous secure-key-elements within the IT and IA space [2]. It has focused on the attackers' side of scenario such as the inspiration at the rear malevolent attacking threats along with the effected factors of human involvement which are related to accidental issues along with the range of observer attacks being performed by the attackers. The ISS based secure real-time parameters prominence on transport collectively and significant obviously an assortment of aspects of IT and IA along with IA based real-time case studies. It can also act as a secure real-time platform for general way of appreciative threats. It can be implicated with the manifestation, modelling the precedent attacks with the secure useful patterns. The ISS can be adopted with new technological tools such as characteristics assessment-based management which has implicated with the authentication set of rules and regulations with the provision of cluster group of policies which govern who-to-access, where-to-access, what-to-access, when-to-access, and level-of-accessibility.

The IT and IA desires to be united with secure layers to scrutinize the technologies which providing the alerting system when data is being accessed illegally from a device to device and device to individual outside with the normal patterns of action. The ISS is providing the technical secure indicators with the employees' characteristic behavioral parameters for assessing the IA an IT based attacks which are performed by the workforce of the EMT. The ISS based secure keys can be classify as significant which the data exists in-stream and accomplish a risk evaluation based

on integrity, privacy, inspection-capability, and accountability. The ISS is showing the technical feasibility to reduce the collision of data breaches whether they are from IT and IA based insiders, hackers, and external attackers.

## 4. Conclusion

The data theft by insiders of the companies is as much the consequence of enterprises failing to execute the scheme and expertise to employee supervise activities and administrate the authenticated data-access to data as it the authentic malicious activities of an employee seeking financial benefits in multi-tenancy environment. This paper has composed with the three major objectives such as: description about the insider attacking types and their impact factors; Description about the prevention of insider attacks and threats; Description about the insider attacks prevention scenario. The prevention is always better than the cure. This paper has described the efficient security scenario to avoid or reduce the insider attaching complexities. This research is more helping the cyber security experts and network administrators to reduce the insider attacks by building the efficient monitoring intelligent system.

## References

[1] Jeremy, Understanding the "Insider Threat" https://cloudtweaks.com/2015/01/4-different-types-attacks-understanding-insider-threat/.

[2] Understanding Insider Threat: A Framework for Characterising Attacks,http://ieeexplore.ieee.org/document/6957307/?reload=true.

[3] Jason R.C. Nurse,, Oliver Buckley, Philip A. Legg, Michael Goldsmith, Sadie Creese, Gordon R.T. Wright, Monica Whitty, Understanding Insider Threat: A Framework for Characterising Attacks, 2014 IEEE Security and Privacy Workshops. http://www.ieee-security.org/TC/SPW2014/papers/5103a214.PDF.

[4] J. Lee, A. Alghamdi and A. K. Zaidi, "Creating a Digital Twin of an Insider Threat Detection Enterprise Using Model-Based Systems Engineering," 2022 IEEE International Systems Conference (SysCon), 2022, pp. 1-7, doi: 10.1109/SysCon53536.2022.9773890.

[5] B. Bowen, M. Ben Salem, S. Hershkop, A. Keromytis and S. Stolfo, "Designing Host and Network Sensors to Mitigate the Insider

Threat," in IEEE Security & Privacy, vol. 7, no. 6, pp. 22-29 (Nov.-Dec. 2009), doi: 10.1109/MSP.2009.109.

[6] P. Dhiman, S. K. Henge, S. Singh, A. Kaur, P. Singh et al., "Blockchain merkle-tree ethereum approach in enterprise multitenant cloud environment," Computers, Materials & Continua, vol. 74, no.2, pp. 3297–3313 (2023).

[7] Dhiman, P.; Henge, S.K.; Ramalingam, R.; Dumka, A.; Singh, R.; Gehlot, A.; Rashid, M.; Alshamrani, S.S.; AlGhamdi, A.S.; Alshehri, A. Secure Token–Key Implications in an Enterprise Multi-Tenancy Environment Using BGV–EHC Hybrid Homomorphic Encryption. Electronics 2022, 11, 1942. https://doi.org/10.3390/electronics11131942.

[8] Alaa Alsaeed, Combating Insider Threats to Enterprise, https://www.academia.edu/37765548/Combating_Insider_Threats_to_Enterprise.

[9] Dou, Z., Khalil, I., Khreishah, A. and Al-Fuqaha, A., 2017. Robust insider attacks countermeasure for Hadoop: Design and implementation. *IEEE Systems Journal*.

[10] Li, W., Meng, W. and Horace, H.S., Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model. *Journal of Network and Computer Applications*, 77, pp.135-145 (2017).

[11] Roy P. and Mazumdar C.. Modelling of Enterprise Insider Threats. DOI: 10.5220/0005327901320136 In Proceedings of the 1st International Conference on Information Systems Security and Privacy (ICISSP-2015), pages 132-136 ISBN: 978-989-758-081-9.

[12] Al-Mhiqani MN, Ahmad R, Zainal Abidin Z, Yassin W, Hassan A, Abdulkareem KH, Ali NS, Yunos Z. A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations. Applied Sciences. 2020; 10(15) : 5208. https://doi.org/10.3390/app10155208.

[13] Walker-Roberts, S.; Hammoudeh, M.; Dehghantanha, A. A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. IEEE Access 2018, 6, 25167-25177.

[14] Nasr, P.M.; Yazdian-Varjani, A. Toward Operator Access Management in SCADA System: Deontological Threats Mitigation. *IEEE Trans. Ind. Inform*. 14, 3314-3324 (2017).

[15] Pitropakis, N.; Lambrinoudakis, C.; Geneiatakis, D. Till All Are One: Towards a Unified Cloud IDS. In Proceedings of the Trust, Privacy and Security in Digital Business; Fischer Hubner, S., Lambrinoudakis, C., Lopez, J., Eds.; Springer: New York, NY, USA, pp. 136-149 (2015).

[16] Al-Mhiqani, M.N.; Ahmad, R.; Yassin, W.; Hassan, A.; Abidin, Z.Z.; Ali, N.S.; Abdulkareem, K.H. Cyber-Security Incidents: A Review Cases in Cyber-Physical Systems. *Int. J. Adv. Comput. Sci. Appl.*, 9, 499-508 (2018).

[17] Liu, L.; De Vel, O.; Han, Q.-L.; Zhang, J.; Xiang, Y. Detecting and Preventing Cyber Insider Threats: A Survey. IEEE Commun. Surv. Tutor., 20, 1397-1417 (2018).

[18] Ullah, F.; Edwards, M.; Ramdhany, R.; Chitchyan, R.; Babar, M.A.; Rashid, A. Data exfiltration: A review of external attack vectors and countermeasures. *J. Netw. Comp. Appl.*, 101, 18-54 (2018).

[19] Ho, S.M.; Kaarst-Brown, M.; Benbasat, I. Trustworthiness Attribution: Inquiry Into Insider Threat Detection. *J. Assoc. Inf. Sci. Technol.*, 69, 271-280 (2018).

[20] Rajamanickam, S. Vollala, S. Amin, R.; Ramasubramanian,N. Insider Attack Protection: Lightweight Password-Based Authentication Techniques Using ECC. IEEE Sys. J. PP, 1-12 (2019).

[21] Li, W.; Meng, W.; Kwok, L.F.; IP, H.H.S. Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model. *J. Netw. Comput. Appl.,* 77, 135-145 (2017).

[22] Callegati, F.; Giallorenzo, S.; Melis, A.; Prandini, M. Cloud-of-Things meets Mobility-as-a-Service: An insider threat perspective. Comput. Secur., 74, 277-295 (2018).

[23] Meryem, A.; Samira, D.; Bouabid, E.O.; Mouad, L. A novel approach in detecting intrusions using NSLKDD database and MapReduce programming. Procedia Comput. Sci., 110, 230-235 (2017).

[24] Lo, O.; Buchanan, W.J.; Griffiths, P.; Macfarlane, R. Distance Measurement Methods for Improved Insider Threat Detection. Secur. Commun. Netw. 2018, 5906368 (2018).

[25] Alizadeh, M.; Lu, X.; Fahland, D.; Zannone, N.; van der Aalst, W.M.P. Linking data and process perspectives for conformance analysis. Comput. Secur. 73, 172-193 (2018).

[26] Harilal, A.; Toffalini, F.; Homoliak, I.; Castellanos, J.H. Twos: A dataset of malicious insider threat behavior based on a gamified competition. J. Wirel. Mob. Netw. (2018) 1.

[27] P. Dhiman, S. K. Henge, "Comparative Analysis of Cloud Security Complexities and Past Proposed Non-Homomorphic and Homomorphic Encryption Methodologies with Limitation" in CRC Press, 4th International Conference on Information and Communication Technology for Competitive Strategies (ICTCS-2019), pp: 787-799, December 13th-14th (2019).

[28] Dhiman, P., Henge, S.K. Analysis of Blockchain Secure Models and Approaches Based on Various Services in Multi-tenant Environment. In: Singh, P.K., Singh, Y., Chhabra, J.K., Illés, Z., Verma, C. (eds) Recent Innovations in Computing. Lecture Notes in Electrical Engineering, vol 855 (2022). Springer, Singapore. https://doi.org/10.1007/978-981-16-8892-8_42.

[29] ArnauErola, IoannisAgrafiotis, Michael Goldsmith, Sadie Creese, Insider-threat detection: Lessons from deploying the CITD tool in three multinational organisations, *Journal of Information Security and Applications,* Vol. 67, 2022, 103167, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2022.103167.

[30] Legg, P. A., Buckley, O., Goldsmith, M., & Creese, S. Automated insider threat detection system using user and role-based profile assessment. *IEEE Systems Journal,* 11(2), 503-512 (2017). https://doi.org/10.1109/JSYST.2015.2438442.