IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

Insider Threats Detection Methods : A Survey

Ujwala Sav[1*], Ganesh Magar[2]

[1]Information Technology, Vidyalankar School of Information Technology, Mumbai, India
[2] Department of Computer Science, S.N.D.T. Women's University, Mumbai, India

[*]*Corresponding Author: ujwalasav@gmail.com, Tel.: +91-9323144955*

DOI: https://doi.org/10.26438/ijcse/v7i4.915923 | Available online at: www.ijcseonline.org

Accepted: 17/Apr/2019, Published: 30/Apr/2019

***Abstract*—** We are living in the age of advanced digital era. We could not even have thought of living without digital gadgets. Almost all the public and private sectors are working with digital data. There is a need to secure this confidential digital data from insider and outsider cyber-attacks. This research paper includes the survey of insider threat detection methods. Insider threats detection are more difficult because insiders are having all privileges or credentials to access the resources and no one will suspect on them. It is easy to transfer the digital data and access can be given to handle this data remotely through compromised insiders. Insider threats results in digital data theft, data leakage and data loss which impacts on profit level and damage the organization image in the market. Survey covers emerging technologies used for detection of insider threats. This research paper identifies the trends of tools, methods used for insider threat detection. It presents information year wise in statistical tabular format. This paper gives insight for future work and challenges to mitigate the cyber-attacks by insider threats.

***Keywords*—**Insider threats, cyber-attacks, detection methods

I. INTRODUCTION

Insider threats are the most dangerous threats in cyber security. There are many researchers are working in this direction to mitigate the insider threats from the system. But most difficult part of the cyber security is to identify the compromised users and machines. Machines are connected to the server or under monitoring. There is no a specific behavior of compromised user so that it will be helpful to identify. There is a need to secure the organization from outsider and insider cyber-attacks. If we protect organization from cyber-attacks, then automatically cyber security will be maintained. Outsider threats can be detected at some level but insider threats are not possible to detect easily. To know more about the research related to insider threats, author conduct literature survey of the recent papers and techniques.

In this paper, researcher has surveyed the research papers in the domain of cyber security and especially of insider threat detection methods or techniques. There are many advanced techniques are introduced in recent years to reduce the insider threats like data mining, internet of things, artificial intelligence, cloud computing, mobile computing, data analytics, etc. Each method is different than other and detects the insider threats at some extent. We need to find out the most effective method. Therefore, there is need to study of the insider threat detection methods and find out the different types of methods which are implemented by different researchers. In their research, which method is applied and which is the specific tool and technique or algorithm is used for insider detection.

The statistical analysis on selected literature is performed. The literatures data is selected from 2008 to 2019. It is arranged in ascending order of year. It identified the methods used and changes in insider threat techniques. Data is arranged and presented in tabular format to know how the detection methodologies are used in every year along with recommendations for future work and study.

Research paper is consists of 6 sections. Section I contains the introduction of insider, insider threats, need of research, contribution and organization of paper, Section II contains the related work of other researchers relevant to the domain and it is summarize, Section III contains the descriptions of methods used for insider detection in brief, Section IV contains the research methodology and data used, Section V describes the result and interpretation of tools, methods and processes, Section VI concludes the research with methods and utilization of it. It describes the limitations and provides suggestions for future research.

II. RELATED WORK

Security is the main aspect for success of organization. Cyber is a very vulnerable area where it is easy to attack and hack the confidential data. In the cyber security, there are number of efforts and research done by researchers. In this section, literatures are surveyed to find out the insider threat detection methods.

In last decade, people have started realizing that there is a need for cyber security as use of mobile and computer has been increased extremely. The experts have taking place research and publishing the research paper in the cyber security domain. Author has included the literatures from 2008 to 2019-time span.

In 2008, article published in journal has mentioned the ten lessons. They are as follow: Measure the right risks, low tech attacks are easier, logs should be checked, don't rely on secrecy for security, privileges are to be given task owner and revoke as and when task is completed, looking at the wrong things, be aware from social engineering, don't believe everything you read, removing staff is risky, Check the background of insiders to minimize the insider attacks and Security measures should be keep on working and monitored [1].

In 2009, to address insider threat, the authors have designed architecture for insider threat detection that combines an array of complementary monitoring and auditing techniques. Survey of 522 security employees from US corporations and government agencies, the annual CSI Computer Crime and Security Survey for 20081 found that 44 percent of respondents cited insider incidents [2].

The most of the trade secrets theft is happened is just because of compromised users and machines. Therefore, MITRE researchers designed a prototype system for identifying insider threats, which prompted a team of engineers and social scientists to experimentally study how malicious insiders use information differently from a benign baseline group [3].

We need to implement the multiple set of strategies which covers the components of taxonomy. It states how the taxonomy, coupled with goals of prevention, detection, mitigation, remediation, and punishment, can suggest sensible and effective response options [4].

The authors provide a systems-based framework and model for understanding important elements, their interactions, interdependencies, and gaps for insider security [5].

In 2010, the research paper discusses a new hypothetical scenario to illustrate the protection that a trust system provides against insider threats [6].

In this paper four examples were discussed related to cyber security, in each example, the resources were put at risk by the actions of people with legitimate access to an organization's information system. Therefore, it has designed the framework which actions posing risks in four areas: the organization, the individual, the information technology(IT) system, and the environment [7].

Rogue devices are an increasingly dangerous reality in the insider threat problem domain. Industry, government, and academia need to be aware of this problem and promote state-of-the-art detection methods [8].

There are end users who don't know the security products and they are reluctant from use of it. In this research paper, introduced web based browser attacks [9]. It is common observation about employees and employer that they are giving least importance to the security aspects.

CADS consists of two components: 1) relational pattern extraction, which derives community structures and 2) anomaly prediction, which leverages a statistical model to determine when users have sufficiently deviated from communities [9].

This work on progress paper proposes a design focused on the notion of increased participation of internet service providers in protecting end users [10].

Web applications are vulnerable to two types of security threats. The first is a request integrity attack. The second is guideline violation, which stems from privilege misuse [11].

In this paper, we propose a framework for modelling the insider-threat problem threats, common precursors, and human actions and behaviors [12].

If activity is normal, then message is generated and if the activity is abnormal then the rule engine checks rules for intrusion. The malicious activity also stored in database for future IDS [13].

There are two static analysis technologies used in this research. 1) Fault Tree Analysis and 2) Finite-State Verification, can be used to identify vulnerabilities to insider attacks upon processes Whereas FTA is a deductive, top-down analytical technique and Finite-State Verification (FSV) is a technology used to infer characteristics about the executions of some or all paths by specified system [14].

Behavioral analysis of insider threat framework is proposed and boot strapping algorithms is used and also developed to produce realistic data [15].

Inside user's behavior can be analyzed and detect intrusion. In order to know that there is a change in the behavior of the user, audit record of the users must be maintained as input to an Intrusion Detection System. In Rule based detection, a certain set of rules are defined that are used to identify normal user or intruder. The rule based Expert system consist set of rules that work like human expert detects intrusions using rules. [16].

There is general tendency of human being to misuse the resources of organization. This system helps to detect publicly available insider threat dataset [17].

A Bayesian Network (BN) is a probabilistic graphical model that represents a set of random variables and their conditional dependencies via a Directed Acyclic Graph (DAG) to reason about uncertainty. The model was tested on sets of data from experts and random data [18].

In this literature BLITHE used to track the insider threats on physical devices. Insider threats are detected using behavior rule based approach and comparative analysis [19].

Cloud storage is to be secured when data shared in group along with insider threat personnel. Security issues can be minimized by secured data sharing techniques [20].

Aspect of honey token is used by using query which provides generic implementation for honey-tokens [21].

A new approach to identify anomalous behavior based on heterogeneous data and a data fusion technique. A new anomaly detection technique which is recently introduced and known as empirical data analytics (EDA) is applied to detect the abnormal behavior based on the datasets [22].

One of the insider threats in cyber security is data leakage. Data leakage prevention (DLP) is a new challenge with large data. Experimental results show that the proposed method can detect leaks of transformed or fresh data fast and efficiently [23].

Data is tremendously increasing on both the side of server and client. Data is large and complex, therefore deep autoencoder is used to detect anomaly. The feature extraction is implemented with a simple frequency based concept, requiring little prior knowledge. Each autoencoder is trained with a specific category of audit data and its optimal model is tuned experimentally [24].

Clustering procedure is used for insider threat detection framework based on unsupervised mining of behavior of inside users. It used publicly available data set composed of truncated Unix commands issued by insiders. Evaluation of the algorithm output, defined as the ability of the algorithm to detect violations of the allowed behavior grouping, is conducted through comparisons with the ground truth provided with the data set used [25].

Combating the insider risks need an understanding of the behavior of each insider. Markov chains (MC) are particularly well suited to model behaviors from network traffic, they were extensively used for modeling and clustering actions.

Data volume is increasing in an extreme basis and social network traffic is continued. Therefore, we need secure transmission of data plays a critical role in realizing all of the key requirements of social multimedia networks. Software Defined Network play a vital role [27].

To enhance the reliability of the SDN, a hybrid deep-learning-based anomaly detection scheme for suspicious flow detection in the context of social multimedia is used [27]. There are two modules. First is anomaly detection module and second one is end-to-end delivery module.

With cloud storage services, users can remotely store their data to the cloud and realize the data sharing with others. Remote data integrity auditing is proposed to guarantee the integrity of the data stored in the cloud [28]. How to realize data sharing with sensitive information hiding in remote data integrity auditing still has not been explored up to now.

III. METHODOLOGY

Authors explored the literatures which are relevant to insider threat detection methodologies. Survey method is used to know about the current scenario and status of insider threats detection methods used for this research paper. The research papers are considered in between 2008 to 2019. These literatures reported the methods, issues, challenges, limitations and scope of insider threat detection method used by that researcher. There are so many research papers in this area. Researcher has arranged the papers in year wise and the most relevant are selected for study.

A. Data Sampling

Literature data is selected relevant to the research study. The selected number of research papers year wise mentioned in the chart given below.

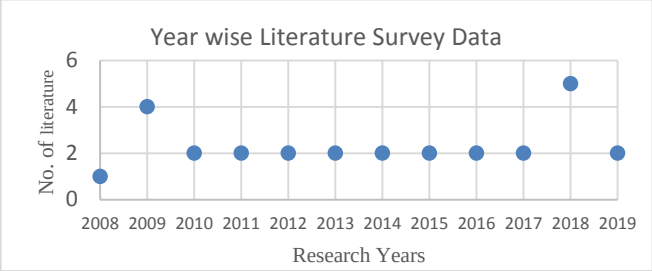

Figure 1. Yearwise Literature Sampling for Survey

IV. INSIDER THREATS AND DETECTION METHODS

There are the threats in terms of outsider and insider users or machine which cause the cyber-attack. Data security is the important aspect for the business success. There are the basic terms used in the research is described as follows.

A. Insider Threats

Insider threats are the machines or users, who are transferring the data to the outsider without having the authorization. There are the machines and users who are compromised and passing the business secretes to the competitors.

B. Insider threats and its impact on business

Business success is the main goal of every organization. The success is depending on well management, resources, exposures and also security. There is a need to secure organization secretes from the competitors in the business. Insiders are the vulnerable in the organization. If insider threat occurs, then there is very serious and huge loss will be there. To avoid these cyber-attacks due to insiders, we need to find out the solution which secure the business secretes from intruders.

C. Advanced Detection Methodology

Machine learning, Deep learning, Internet of Things and Cloud computing is the latest technology used to handle large and complex data. The brief description of the technology is given below.

1) Cloud Computing

A novel automated approach combining two modules FESNA and ESMA is developed and simulated for log analysis. It helps to predict and identify intrusion along with its intruder by analysing cloud network and management log. As a result of the identification phase a forensic identification report FIR is also generated to drive the further forensic analysis Smoothly [29].

2) Machine Learning

The machine learning is a very vast field of computer science in modern technology, through the availability of internet. Supervised and unsupervised algorithms can be used by the researchers. Their algorithms types are given below.

a) Supervised SL algorithms.[30]

- Naïve Bayes (NB).
- Logistic Regression (LR).
- Support Vector Machines (SVM).
- Random Forest (RF).
- Hidden Markov Models (HMM).
- K-Nearest Neighbor (KNN).
- Shallow Neural Network (SNN).

b) Unsupervised SL algorithms

- Clustering.
- Association

3) Deep Learning

All DL algorithms are primarily based on Deep Neural Networks (DNN), which can be big neural networks organized in many layers able to self-sufficient representation learning [30].

- Fully-connected Feedforward Deep Neural Networks(FNN)
- Convolutional Feedforward Deep Neural Networks (CNN)
- Stacked Auto Encoders(SAE)
- Deep Belief Networks (DBN)

D. Limitations of present system

If the attacker is an insider in that case we suggest a different security level that is face recognition after login. If system finds some mismatch then return decoy information to user. Sometime service providers can be an attacker in that case it is difficult to identify attacker but we can confuse him using decoy technique.

De-merits of existing system 1. We can't detect when data attack happened 2. We can't detect person behind that attack. 3. We can't detect which file was hacked [31].

E. Role of Cyber Security

The development on Information Security Management System (ISMS) had a long development history in any organization and low adoption of ISO 27001 was observed. The high costs in money and time of ISMS implementation are definite barriers for smaller size companies to adopt the standard [32].

V. RESULTS AND DISCUSSION

Authors have studied the research and find out the insider threat detect methods and its utilization. The findings are presented in tabular form. This tabular form is helpful to know about the development in the research in the area of insider threats prevention and detection to provide cyber security.

A. Literature Data Analysis

Researchers have analyzed the data and presented in the tabular form. The standard journals and conferences like IEEE, IJCSE and Research gate are refered for this study. Most of the literatures are from journal with detail study. Total no. research papers are surveyed are 32 whereas 4 are from IJCSE journals.

Insider threat detection can be performed by number of ways. The insider threat detection methods development is shown in the table given below.

Table 1: Insider threats detection methods 2008 onwards

Year	Methodology	Recommendation
2008	Preventive measures ten lessons described to avoid insider threats.	Security measures should be on and monitored.
2009	Architecture for monitoring and detecting insider attacks. Host-based sensors monitor user activity to detect malicious users masquerading as other system users. Trap-based decoys attempt to catch attackers who use their own legitimate credentials [2]. The sensors are collecting the data and analysis the anomalous actions.	It is useful to detect the malicious actions of inside users.
	The Elicit (Exploit Latent Information to Counter Insider Threats) system. Elicit examines how users interact with information, applying contextual information to identify suspicious behaviors. It then combines all observed behaviors into a single threat score to help analysts prioritize their investigations [3].	This research gives insights about how malicious user behaves in the organization.
	Framework for taxonomy of insiders and their actions. This taxonomy provides a consistent vocabulary for describing which aspects of the insider threat are being addressed, and takes into account the roles of organizations, individuals, IT systems, and the environment in enabling insider threat behavior[4].	Framework can be applied for insider threat mitigation.
	System dynamics model is consisting of two sub models. The first one is employee life-cycle model, shows the evolution of insiders within an organization and the second is the information access model which represents how employees have legitimate access to protected information as needed to do their jobs or how a malicious insider would gain illicit access to protected information [5].	This model helps to understand insider's interactions, interdependencies and gap in insider threat detection system.
2010	Trust system models and configuration options [3 [6].	The trust system provides comprehensive logon state and security situational awareness.
	Insider threat framework and Questions pertaining to insider threat framework [7].	It is describing and differentiating the types of insider threats. Framework will improve the insider threat detection.
2011	Wired-side method for	RAP is shown the

	rogue-access-point (RAP) detection that's rooted in the 802.11 MAC (media access-control) protocol's functionality [8].	effectiveness
	The proposed design takes advantage of three different detection tools to identify the maliciousness of website content and alerts users through utilizing Internet Content Adaptation Protocol (ICAP) by an In-Browser cross-platform messaging system [9].	This system analysis the online behavior of users.
2012	It detects anomalous user behaviors based on the sequence of their requests within a web session. Next, we apply a hidden Markov model (HMM) to characterize workflows on a per-object basis [10].	The clustering approach can achieve relatively low false positive rates along with accuracy.
	It has used community anomaly detection system (CADS), an unsupervised learning framework to detect insider threats based on the access logs of collaborative environments [11].	This model is useful for detecting the insider threats based on access logs of collaborative environment.
2013	Conceptual Model and Reasoning Structure. It identifies insider who has threatening behavior towards an organization. Reasoning can be performed on elements within the real world [12].	It provides encompassing view to detect insider threats.
	A hybrid classification approach of Support Vector Machine (SVM) and Gravitational Search Algorithm (GSA) algorithm used to enhance the detection accuracy [13].	A hybrid machine learning model based on combining the unsupervised and supervised classification techniques used.
2014	Process model and analysis the detection [14]	Countermeasures are implemented.
	Survey y is conducted and develops BAIT algorithms and supervised learning algorithms [15].	In future, psychological testing, NLP with behavioral analysis is required.
2015	The rule based expert system used to detect the behavior of the insider intrusion. [16].	The malicious activity stored in database and help to detect for future IDS.
	It provides generic implementation for honey tokens [17].	This is used to reduce the problems of honey tokens.
2016	Cyber security belief network is used in order to facilitate frameworks execution thus it helps in reducing threats [18].	This model studies the relation of inter-related cyber security parameters.
	A behavior rule-based methodology for insider threat (BLITHE) detection is data monitor devices in smart grid. Specifically, a rule-weight and compliance-distance-based grading strategy is designed [19].	BLITHE is detecting anomalous behavior in smart grid applications.
2017	Secure Data Sharing in Clouds (SeDaSC) methodology that provides: 1) data confidentiality and integrity; 2) access control; 3) data sharing (forwarding) without using compute-intensive re-encryption; 4) insider threat security; and 5) forward and backward access control [20].	SeDaSC secure the data sharing in the cloud.
	It presents a scalable system for high-throughput real-time analysis of heterogeneous data streams [21].	RADISH performs predictive analytics and malicious data into the system.
2018	Heterogeneous data which combine all the data from the VAST Challenge as well as image data used in data fusion technique. These can assist the human expert in processing huge amount of heterogeneous data to detect anomalies [22].	In future research, text data can also be used as a part of heterogeneous data mixture, and the data fusion technique may be applied to other datasets.
	An adaptive weighted graph walk model to solve data leakage problem by mapping it to the dimension of	Data leakage problem is resolved with the help of adaptive

	weighted graphs. Label propagation is used to enhance the scalability for fresh data. Finally, a low-complexity score walk algorithm is used [23].	weighted graph.
	Auto encoder based anomaly detection is used [24].	This system able to detect all of the malicious insider actions with a reasonable false positive rate
	Clustering algorithms are used to detect the insider threats[25]	Clusters are used. Use principal component analysis for good results.
	Markov process to model profiles for individual users rather than modeling actions is used [26].	Temporal component stream clustering adapted.
2019	An anomaly detection module improved restricted Boltzmann machine and gradient descent-based support vector machine to detect the abnormal activities, and 2) an end-to-end data delivery module to satisfy strict QoS requirements of the SDN, that is, high bandwidth and low latency[27].	It is evaluated on real time and bench mark dataset to show effectiveness of anomaly detection.
	A remote data integrity auditing scheme that realizes data sharing with sensitive information hiding to sanitize the data blocks corresponding to the sensitive information of the file and transforms these data blocks' signatures into valid ones for the sanitized file. Signatures are used to verify the integrity of the sanitized file in the phase of integrity auditing [28].	Sensitive information is remain hidden, while the remote data integrity auditing is enable to be efficiently executed

B. Trend of Insider Threats detection methods

On the basis of survey, it is observed that there is change in the technology and according change in the detection methods as per the timeline. Timeline for study is considered from 2008 to 2019. It helpful to know about the current research and need of research in future. The timeline of the methods are in the chart given below.

Table 2: Changing Trend of Insider Threat Detection Methods

Year	**Methodology Observed**
2008	Security lessons
2009	Sensor based architecture for Monitoring
	Exploit Latent Information to Counter Insider Threats
	Framework Taxonomy
	Employee cycle and Information access model
2010	Trust system model
	Threat framework
2011	Rogue access point detection
	Internet Content Adaptation Protocol (ICAP)
2012	Hidden Markov model (HMM)
	Unsupervised learning framework
2013	Conceptual Model and Reasoning Structure
	hybrid machine learning model using SVM and GSA
2014	Process Model
	Supervised learning algorithms
2015	Rule based expert system
	Generic implementation for honey tokens
2016	Belief network
	BLITHE) detection is data monitor devices in smart grid
2017	Secure Data Sharing in Clouds (sedasc) methodology
	Analysis of heterogeneous data streams
2018	Data fusion technique
	Adaptive weighted graph walk model
	Autoencoder
	Clustering algorithm
	Markov process model
2019 till date	remote data integrity auditing scheme
	Boltzmann machine and gradient descent-based support vector machine

VI. CONCLUSION AND FUTURE SCOPE

This research paper concludes that there is a need to protect the organization from outsider threat as well as insider threats. Many insider threat detection systems have been developed in last decade but still there is a scope to work in this domain. Due to compromised user, hackers or competitors are easily get access to the digital confidential organization data. Innovative techniques used by researchers to minimise the risk from insider threats and to secure the business secrets.

It is studied that technology is changing with time. Due to advance technology and digitization volume of data, number

of users, number of applications, number of vulnerabilities, data breaches and cyber-attacks are increasing. Hence researchers are also starting from training and awareness program to users to deep learning automated detection methods have been developed. There is a future scope to find out the optimized research method to remove the insider threats before getting into serious problems in the organization.

REFERENCES

[1] J. Epstein, "Security Lessons Learned from Society," *IEEE Secur. Priv. Mag.*, vol. 6, no. 3, pp. 80–82, May 2008.

[2] B. M. Bowen, M. Ben Salem, S. Hershkop, A. D. Keromytis, and S. J. Stolfo, "Designing Host and Network Sensors to Mitigate the Insider Threat," *IEEE Secur. Priv. Mag.*, vol. 7, no. 6, pp. 22–29, Nov. 2009.

[3] D. Caputo, M. Maloof, and G. Stephens, "Detecting Insider Theft of Trade Secrets," *IEEE Secur. Priv. Mag.*, vol. 7, no. 6, pp. 14–21, Nov. 2009.

[4] S. L. Pfleeger and S. J. Stolfo, "Addressing the Insider Threat," *IEEE Secur. Priv. Mag.*, vol. 7, no. 6, pp. 10–13, Nov. 2009.

[5] F. Duran, S. H. Conrad, G. N. Conrad, D. P. Duggan, and E. B. Held, "Building A System For Insider Security," *IEEE Secur. Priv. Mag.*, vol. 7, no. 6, pp. 30–38, Nov. 2009.

[6] G. M. Coates, K. M. Hopkinson, S. R. Graham, and S. H. Kurkowski, "A Trust System Architecture for SCADA Network Security," *IEEE Trans. Power Deliv.*, vol. 25, no. 1, pp. 158–169, Jan. 2010.

[7] S. L. Pfleeger, J. B. Predd, J. Hunker, and C. Bulford, "Insiders Behaving Badly: Addressing Bad Actors and Their Actions," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 1, pp. 169–179, Mar. 2010.

[8] R. Beyah and A. Venkataraman, "Rogue-Access-Point Detection: Challenges, Solutions, and Future Directions," *IEEE Secur. Priv. Mag.*, vol. 9, no. 5, pp. 56–61, Sep. 2011.

[9] M. Mansoori and Ray Hunt, "An ISP Based Notification and Detection System to Maximize Efficiency of Client Honeypots in Protection of End Users," *Int. J. Netw. Secur. Its Appl.*, vol. 3, no. 5, pp. 59–73, Sep. 2011.

[10] Y. Chen, S. Nyemba, and B. Malin, "Detecting Anomalous Insiders in Collaborative Information Systems," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 3, pp. 332–344, May 2012.

[11] X. Li, Y. Xue, and B. Malin, "Detecting Anomalous User Behaviors in Workflow-Driven Web Applications," 2012, pp. 1–10.

[12] P. Legg *et al.*, "Towards a Conceptual Model and Reasoning Structure for Insider Threat Detection," p. 19, 2013.

[13] S. Omar, A. Ngadi, and H. H. Jebur, "An Adaptive Intrusion Detection Model based on Machine Learning Techniques," *Int. J. Comput. Appl.*, vol. 70, no. 7, pp. 1–5, May 2013.

[14] M. Bishop *et al.*, "Insider Threat Identification by Process Analysis," in *2014 IEEE Security and Privacy Workshops*, San Jose, CA, 2014, pp. 251–264.

[15] A. Azaria, A. Richardson, S. Kraus, and V. S. Subrahmanian, "Behavioral Analysis of Insider Threat: A Survey and Bootstrapped Prediction in Imbalanced Data," *IEEE Trans. Comput. Soc. Syst.*, vol. 1, no. 2, pp. 135–155, Jun. 2014.

[16] Z. Malek and D. B. Trivedi, "The Rule Based Intrusion Detection Model for User Behavior," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, p. 4, 2015.

[17] K. Padayachee, "Aspectising honeytokens to contain the insider threat," *IET Inf. Secur.*, vol. 9, no. 4, pp. 240–247, Jul. 2015.

[18] I. Atoum and A. Otoom, "Effective Belief Network for Cyber Security Frameworks," *Int. J. Secur. Its Appl.*, vol. 10, no. 4, pp. 221–228, Apr. 2016.

[19] H. Bao, R. Lu, B. Li, and R. Deng, "BLITHE: Behavior Rule-Based Insider Threat Detection for Smart Grid," *IEEE Internet Things J.*, vol. 3, no. 2, pp. 190–205, Apr. 2016

[20] M. Ali *et al.*, "SeDaSC: Secure Data Sharing in Clouds," *IEEE Syst. J.*, vol. 11, no. 2, pp. 395–404, Jun. 2017.

[21] B. Bose, B. Avasarala, S. Tirthapura, Y.-Y. Chung, and D. Steiner, "Detecting Insider Threats Using RADISH: A System for Real-Time Anomaly Detection in Heterogeneous Data Streams," *IEEE Syst. J.*, vol. 11, no. 2, pp. 471–482, Jun. 2017.

[22] A. M. Ali and P. Angelov, "Anomalous behaviour detection based on heterogeneous data and data fusion," *Soft Comput.*, vol. 22, no. 10, pp. 3187–3201, May 2018.

[23] X. Huang, Y. Lu, D. Li, and M. Ma, "A Novel Mechanism for Fast Detection of Transformed Data Leakage," *IEEE Access*, vol. 6, pp. 35926–35936, 2018.

[24] L. Liu, O. De Vel, C. Chen, J. Zhang, and Y. Xiang, "Anomaly-Based Insider Threat Detection Using Deep Autoencoders," in *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, Singapore, Singapore, 2018, pp. 39–48.

[25] S. Elshafei and A. Abdelnaby, "Using semantic variations in clustering insiders behavior," in *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, Antalya, 2018, pp. 1–5.

[26] M. Dahmane and S. Foucher, "Combating Insider Threats by User Profiling from Activity Logging Data," in *2018 1st International Conference on Data Intelligence and Security (ICDIS)*, South Padre Island, TX, 2018, pp. 194–199. [26] Yakubu Ajiji Makeri, "The role of Cyber Security and Human-Technology Centric for Digital Transformation", International Journal of Scientific Research in Computer Science and Engineering, Vol.6, Issue.6, pp.53-59, 2018.

[27] S. Garg, K. Kaur, N. Kumar, and J. J. P. C. Rodrigues, "Hybrid Deep-Learning-Based Anomaly Detection Scheme for Suspicious Flow Detection in SDN: A Social Multimedia Perspective," *IEEE Trans. Multimed.*, vol. 21, no. 3, pp. 566–578, Mar. 2019.

[28] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, "Enabling Identity-Based Integrity Auditing and Data Sharing With Sensitive Information Hiding for Secure Cloud Storage," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 2, pp. 331–346, Feb. 2019.

[29] P. Santra, "An Expert Forensic Investigation System for Detecting Malicious Attacks and Identifying Attackers in Cloud Environment", International Journal of Scientific Research in Network Security and Communication, Vol.6, Issue.5, pp.1-26, 2018.

[30] Afzal Ahmad, Mohammad Asif, Shaikh Rohan Ali, "Review Paper on Shallow Learning and Deep Learning Methods for Network security", International Journal of Scientific Research in Computer Science and Engineering, Vol.6, Issue.5, pp.45-54, 2018.

[31] Poonam Devi , "Attacks on Cloud Data: A Big Security Issue", International Journal of Scientific Research in Network Security and Communication, Vol.6, Issue.2, pp.15-18, 2018.

[32] Yakubu Ajiji Makeri, "The role of Cyber Security and Human-Technology Centric for Digital Transformation", International Journal of Scientific Research in Computer Science and Engineering, Vol.6, Issue.6, pp.53-59, 2018.

Authors Profile

Mrs. Ujwala M. Sav holds a Bachelor degree in Computer Science, Master degrees in M.Sc. (CS), M.Ed., MBA(Marketing), M.Phil (IT), along with Diploma in Business Management and Diploma in Marketing Management. She is currently working as Assistant Professor in Department of Information Technology at Vidyalankar School of Information Technology, Wadala, Mumbai. She is currently pursuing her Ph,D. from S.N.D.T Women's University, Mumbai. She is a life member of Computer Society of India. Her research work focused in Cyber Security and Machine Learning. She has more than 15 years of teaching experience in computer science and information technology courses.

Dr. Ganesh M. Magar holds Bachelor and Master degrees in Computer Applications and also a Doctorate degree in Computer Science. He is currently working as Associate Professor Head in P.G. Department of Computer Science and (Ad-hoc) Dean, Faculty of Science and Technology at S.N.D.T. Women's University, Mumbai. He is a member of IEEE, ACM, ISCA, CSI and many others scientific societies. He has published more than 20 research papers in peer-reviewed reputed international journals and conferences. His thurst research areas include GIS, databases and image processing. He has more than 16 years of teaching and research experience and 3 years of Industry Experience.

