IDENTIFICATION OF INSIDER THREAT IN A CLOUD-BASED SYSTEM- A REVIEW

Mrs. R Reshma Ramesh [1], Prof. Raj Kumar T. [2] and Dr. Sobhana N V [3]

[1] *M.Tech Cyber Forensics & Information Security, College of Engineering, Kallooppara, Pathanamthitta, Kerala, India*
[2] *Department of Computer Science and Engineering, College of Engineering, Kallooppara Pathanamthitta, Kerala, India*
[3] *Department of Computer Science and Engineering, Rajiv Gandhi Institute of Technology Velloor P O, Pampady, Kottayam*
[1] *reshmaramesh225@gmail.com,* [2] *rajcek@gmail.com,* [3] *sobhana.nv@gmail.com*

Abstract: *Cloud computing bought about an incredible overhaul of the phenomenon of companies having to put in significant capital investments to build software and IT infrastructure. It assurances to help organizations save money on IT expenditure while increasing reliability, efficiency, and productivity. However, despite the potential benefits that the cloud promises its users, it is facing some security issues like data loss, insider threat, outsider threat, data breaches, malware injection, etc. Still, insider threats persist as one of the major concerns because insider threat is a security risk to an organization that comes from within the business itself. Although the number of insider threats is much lower than external network attacks, insider threats can cause widespread damage. As insiders are very aware of an organization's system, it is very difficult to detect their malicious behavior. In this paper, we propose the need of insider-threat detection methods based on user behavior modeling and anomaly detection algorithms such as Binary classification and Logistics Regression algorithm to detect malicious activities.*

Keywords: **cloud computing, security issues, insider threat, behavioral modeling.**

1. INTRODUCTION

Malicious activities are external threats to the network. They are activities performed by cybercriminals that infiltrate your system to steal sensitive information, sabotaging your operations, or doing damage to your hardware or software. Malware analysis is a diverse field where it is becoming increasingly difficult to keep continuous track of malicious activities that deviate inter-character and method of operation. Insider threats are malicious activities by authorized users, such as theft of intellectual property or security information, fraud, and sabotage [1]. Although the number of insider threats is much lower than external network attacks, insider threats can cause widespread damage.

As insiders are very acquainted with an organization's system, it is very difficult to detect their malicious behavior. One of the largest challenges at intervals the event of resilient and secure cloud-oriented mechanisms is expounded to the suitable recognition of malware. While Data and applications are moving to the cloud environments can enlarge businesses, malicious sabotage of an organization's sensitive information resources could threaten the entire victim organization's operation.

2. CLOUD COMPUTING AND FORENSICS

Cloud computing has shaped the abstract and infrastructural basis for tomorrow's computing [2]. The global computing infrastructure is quickly moving regarding the cloud-based design thus it's necessary to require advantage of cloud-based computing through deploying in wide-ranging sectors that the security aspects in a very cloud-based atmosphere stay at the core of interest. Cloud-based services and service providers are being evolved which has resulted in a new business trend based on cloud technology [2].

Cloud computing is estimated to be the most transformative technology in the history of computing. Cloud organizations, which contain the providers and customers of cloud services, have yet to create a well-defined forensic capability. Without this, they are incapable to ensure the robustness and suitability of their services to

support investigations of criminal activity. Cloud computing is a new battlefield of cybercrime, as well as a new ground for novel investigative approaches [3].

Cloud Forensics is a truly associate application inside Digital Forensics that oversees the crime committed over the cloud and investigates thereon. Cloud computing relies on a large network, that spreads globally. Therefore, Cloud Forensics is claimed to be a set of NetworkForensics.

The cloud service provider and also the customers have nevertheless to establish forensic capabilities which will support the investigation just in case if any crime is committed. The Technical Dimension consists of tools that are needed to execute the forensics investigations in Cloud Computing. These consist of information or data assortment, live forensics, proof partition, and virtualized environments.

3. RELATED WORK

This section will survey the methods from various areas that we consider as the insider threat detection methods.
Akhil Behl [4] suggested the security challenges in the cloud and has tried to address the most common and critical ones. The cloud infrastructure security issues and the different malicious threats that can affect the cloud infrastructure elements were addressed. The key research challenges for implementing security solutions to protect the cloud-based infrastructure were also explored.
Junhong Kim et al. [1] recommended the insider-threat detection methods using user behavior modeling based on user log datasets such as user's daily activity summary, user's weekly e-mail communication history, and e-mail contents topic distribution. Anomaly detection algorithms such as one class classification algorithm and their combinations are then applied to detect malicious activities.
N. Nguyen [6] proposed the insider threat detection method based on buffer overflow. And by now, only a few kinds of research have been done. Besides, limited by test environment and real test data, studies on internal threat detection also lacks unified and effective metrics to measure their efficiency.
Xuebin Wang et al. [5] proposed a new data-centric approach to find malicious insider threats that supported characterizing user behavior by extracting the features of user interaction behavior as well as keystroke dynamics and consecutive queries to model users' access patterns. Statistical learning algorithms are trained and tested from the dataset to predict abnormal behavior patterns; experimental results indicate that the approach is incredibly effective and correct.

4. SECURITY ISSUES IN CLOUD

Cloud computing provides organizations with an efficient, flexible, and cost-effective alternative to hosting their computing resources [4]. Information Security in cloud storage may be a key dread with regards to the degree of trust and cloud penetration [7]. In a cloud-based system, security is shared between the cloud provider and the user. To a definite limit, adopting Cloud computing has struggled to grow among several established and growing organizations because of security and privacy-related issues [8]. Many security activities are occurring inside or outside of the cloud services provider's/consumer environment. Therefore it can be broadly classified as Insider threat, outsider threat, Loss of data, Privacy of data, lack of visibility, issues related to multi-tenancy, loss of control, and Disruption of service.

a. Insider Threat

An insider threat is a malicious activity to an organization that comes from the person within the organization, such as employees, former employees, contractors, who have inside information concerning the organization's security follows, data, and computer systems.

b. Outsider Threat

Outside threats are one of the most important issues with any organization since it directly entails the release of confidential sensitive information out in open or spoiling the organizations. These attacks follow a typical series of seven activities: Malware Introduction, Command and management, Malware enlargement, Target Identification, Exfiltration, Planning, and Retreat or Removal.

c. Loss of Data

Data loss is a miscalculation condition in data systems during which data is destroyed by failures or neglect in storage, transmission, or process. Information systems implement backup and disaster recovery instrumentation and processes to restore lost information or data.

d. Privacy of Data

Data privacy and confidentiality could be major concerns for several organizations. Several Organizations have adopted cloud computing. However they lack the data to make sure that they and their staff area unit victimized it firmly. As a result, sensitive data is at risk of contact – as confirmed by a huge number of cloud data breaches.

e. Lack of Visibility

An organization's cloud-based resources are placed outside of the company network and run on infrastructure that the corporate doesn't own. As a result, several ancient tools for achieving network visibility aren't effective for cloud environments, and a few organizations lack cloud-focused security tools. This can limit the Associate organization's ability to watch its cloud-based resources and shield them against attack.

f. Issues Related to Multi-Tenancy

Multi-Tenancy is once many various cloud customers are accessing identical computing resources, like once many various companies or organizations are storing data on a regular physical server. As a Cloud is primarily meant to serve multiple users it directly implies that completely different users among a cloud share constant applications and therefore the physical hardware to run their Virtual Machines (VMs) [4].

g. Loss of Control

Loss of control occurs when clients lose their control over their resources in the hand of the service provider. As scarcity of authentication and access management placed by suppliers, loss of management contributes to larger security considerations.

h. Disruption of Service

Cloud Outage merely refers to the length once the cloud infrastructure service is unprocurable to be used. This threat is alleviated by a many-fold method. The provider must employ a strong two-factor authentication technique wherever possible to ensure that its tenants are only getting in after a strong authentication process [4].

5. INSIDER THREAT

This section describes the discussion on the relevant topic of interest to us. Insider threat may be a security issue that arises from persons who have access to a company network, systems, and data, like workers and trusty partners [1]. One of the largest security challenges currently facing all organizations is the "insider threat": either caused accidental or caused by a malicious activity by another person with access to their network. When attackers gain insider access they'll keep unseen among the network for months and cause real and everlasting harm. The main two types of insider threats are malicious insiders (turncloaks) and unwilling participants, severally (pawns).

a. Turncloaks

A turncloak is a malicious and a disloyal insider who is stealing data or sensitive information. In most cases, it's an employee, worker, or contractor – somebody who is meant to get on the network and has legitimate credentials however is abusing their access for fun or profit.

b. Pawns

A pawn is simply a standard employee – a helper who makes an error that's exploited by a nasty actor or otherwise ends up in information loss or compromise. Whether or not may be a lost laptop or computer, erroneously emailing a sensitive document to the incorrect person.

Other types of insider threat are:

c. Malicious Insider

An employee or contractor who is wittingly appeared to steal data or disrupt operations. This might be an opportunist trying to find ways in which to steal data or information that they'll sell or which may facilitate them in their career, or a dissatisfied employee or worker trying to find ways in which to harm an organization, penalize their leader.

d. Negligent Insider

An employee or a business partner who doesn't follow correct IT procedures. For instance, somebody who leaves their PC or computer without shutting down or an administrator who is failed to amend a default password or didn't apply a security patch.

e. Compromised Insider

A common example is a worker or employee whose system or laptop has been infected with malware. This generally happens via phishing scams or by clicking on links that will sometimes download malware codes. There are many means that a worker or employee will become a compromised malicious insider.

f. Phishing

It may be a crime within which a target individual is contacted via email or text message by somebody. They move as a legitimate establishment to entice the individual by providing sensitive information, like in-person distinctive data (PII), banking, and credit card information and passwords. Malware infection is a cybercrime when a machine is infected with malicious software – malware that would infiltrates your computer. The goal of malware within the case of a compromised malicious insider is to steal sensitive data or user credentials such as user id and passwords. Malware infection may be originated by clicking on a link, downloading a file, or plugging in an infected or damaging USB, among different ways. Credential theft is a cybercrime by stealing the username and password – the login credentials – of a targeted person. Credentials theft can be done in a variety of ways such as phishing, social engineering, and malware infection. Pass-the-hash is an advanced form of credential theft where the hashed – encrypted or digested – authentication credential is captured from one computer and used to gain access to other computers on the network.

Insider threats in cloud computing are increasing. Insiders will be simply causing a lot of cyber threats to organizations than outside attackers, for the plain reason—they're already within it. Insider threat detection is a complex and challenging problem because the external expression of internal attack is diverse [5]. Insider threats are present in some industries such as medical hospitals, the money sector, and government establishments — however, they'll compromise the data or information security of any company.

6. COMPARATIVE STUDY OF INSIDER THREAT IDENTIFICATION

Table 1. Identification of insider threat -A Comparative Study

Sl No	Paper Title/ Author	Pros & Cons	Findings
1	**Insider Threat Detection with Face Recognition and KNN User Classification**. M Subrahmanya Sarma, Dr. Y Srinivas et al.	To ensure the detection of Insider threat, it was recommended to make use of face recognition only for the possibly not legitimate or for not legitimate categories. In KNN classification accuracy depends on the quality of data.	Face Recognition is very costly, so need to find a cost-effective method.
2	**Insider Threat Detection Based On User Behavior Modeling And Anomaly Detection Algorithms** Junhong Kim, Minsik Park, Haedong Kim, Et Al	Insider-threat detection framework based on user behavior modeling and anomaly detection algorithms using the CERT dataset. When applied to a real-world dataset, an oversized variety of input variables typically degenerate the model performance due to the high dependency between input variables (multi-collinearity) and also the existence of noise.	This approach can detect the behaviors based on the batch process but cannot detect them in real-time. Therefore a real-time detection method is necessitated.
3	**Insider Threat Detection Using Characterizing User Behavior** Xuebin Wang Qingfeng Tan, Jinqiao Shi, Shen Su and Meiqi Wang	This data-centric approach makes that only interior data usage is monitored which gives rise to low system load. Does not specify the dependency between the user behavior characteristics and distinguishability of different specific users.	This approach experiments only in open source datasets not applicable in the real world.
4	**Insider Threat Detection Model for the Cloud** Lucky Nkosi, Paul Tarwireyi and Matthew O Adigun	This system aaproach uses sequential rule mining to detect malicious usage patterns for a particular profile and help to reduce the false positive and negative rates. Less accurate and Scalable.	This method focused only on SaaS layers so need to find a method that can be applied to IaaS layers, PaaS layers, and IT Systems.

7. CONCLUSION AND FUTURE SCOPE

Mainly insider threat is a security risk that originated from the targeted company/organization involves a current or former employee or business associate who has access to sensitive information and data within the organization's networks. Insider threats are more difficult to identify or block than outsider threats and it is invisible to firewall and intrusion detection systems. The consequences of insider threats will affect the confidentiality and security of sensitive information within an organization. Nowadays insider threats detection mechanism in the cloud is very rare. Some of the insider threat detection methods are behavior pattern, KNN classification, and Face recognition methods.

The problems of these methods are it provides only two-factor authentication, less security, high cost, not applicable in the real world. There are some sophisticated methods which uses Face detection methods but are costly. Some

methods can be employed to open source datasets but cannot be applied in real world environment. There are also some other methods which were restricted to SaaS platform but can't be applied to other Platforms. Hence there is a need for an insider threats detection method that offers more confidentiality, security, low cost and applicable in the real world. In the future, a Standard insider threat detection software or tool can be proposed for the identification of threats in a cloud-based system, which should be accurate in real-time. Latest technologies like AI(Artificial Intelligence) can be used to identify insider threats better than others.

REFERENCES

[1] *Junhong Kim, Minsik Park, Haedong Kim, Suhyoun Cho, and Pilsung Kang, "Insider Threat Detection Based on User Behavior Modeling and Anomaly Detection Algorithms," 25 September 2019.*

[2] *Monjur Ahmed1 and Mohammad Ashraf Hossain2, "Cloud Computing and Security Issues in the Cloud," International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.*

[3] *Keyun Ruan, Prof. Joe Carthy, Prof. Tahar Kechadi, Mark Crosbie, "Cloud forensics: An overview," on 21 May 2014.*

[4] *Akhil Behl, "Emerging Security Challenges in Cloud Computing," 978-1-4673-0126-8/11/$26.00 c 2011 IEEE.*

[5] *Xuebin Wang∗†‡, Qingfeng Tan§, Jinqiao Shi∗†, Shen Su§, and Meiqi Wang, "Insider Threat Detection Using Characterizing User Behavior," 2018 IEEE Third International Conference on Data Science in Cyberspace.*

[6] *N. Nguyen, P. Reiher, and G. H. Kuenning, "Detecting insider threats by monitoring system call activity," in Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society. IEEE, 2003, pp. 45–52.*

[7] *M Subrahmanya Sarma, Dr. Y Srinivas et al, "Insider Threat detection with Face Recognition And KNN User Classification," 2017 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM).*

[8] *Nabeel Khana, Adil Al-Yasiri, "Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework," The 2nd International Workshop on Internet of Thing: Networking Applications and Technologies (IoTNAT' 2016)*

[9] *Lucky Nkosi, Paul Tarwireyi and Matthew O Adigun, "Insider Threat Detection Model for the Cloud," in 2013 IEEE*