A review on Insider Threats Detection and Prevention Techniques: Analysis, Taxonomy and Challenges

1st Dr. A.K.M. Muzahidul Islam
Dept. of Computer Science Engineering
United International University
Dhaka, Bangladesh
muzahid@cse.uiu.ac.bd

2nd Imtiaaze Mahmud
Dept. of Computer Science Engineering
United International University
Dhaka, Bangladesh
imahmood202039@mscse.uiu.ac.bd

3rd Md. Ashique Mostofa Chowdhury
Dept. of Computer Science Engineering
United International University
Dhaka, Bangladesh
mchowdhury211062@mscse.uiu.ac.bd

4th Md. Anisur Rahman
Dept. of Computer Science Engineering
United International University
Dhaka, Bangladesh
mrahman202047@mscse.uiu.ac.bd

5th Abdulkadir Gedi
Dept. of Computer Science Engineering
United International University
Dhaka, Bangaldesh
agedi212060@mscse.uiu.ac.bd

6th Md. Redaan
Dept. of Computer Science Engineering
United International University
Dhaka, Bangladesh
mredaan211009@mscse.uiu.ac.bd

***Abstract*—Cloud computing is a new computing paradigm that enables businesses to use IT without incurring significant upfront costs. The recent introduction of cloud computing has altered everyone's perception of infrastructure designs, software delivery, and development methodologies. Despite the obvious advantages of cloud computing, security remains a key worry, limiting cloud adoption. When considering an insider attack, the term "malevolent insider" comes to mind, yet a malicious insider is one of the organization's legitimate users. Based on his or her job, a valid user inside the company normally gets access to an extraordinary amount of information on a much larger scale. Insider threat, categorization, and relevance to specific cloud environments are discussed here so that we may be prepared with the greatest protection. We have decided to motivate our review paper to detect insider attacks and prevent insider attacks in cloud computing. The goal of our research is to identify and create a taxonomy of insider attack and its defenses.**

***Index Terms*—cyber security, cloud computing, insider attack, insider attack detection.**

I. Introduction

Among other cyber threats, insider attacks are the key threat to different kinds of organizations not excluding governments. Recently we can see several kinds of data leaks which affect each organization's reputation. Wikileaks, Stuxnet, Sony attack and so on are the most dangerous insider attacks that have been performed in recent days [1]. Private companies, govt. Organizations, Media houses and socially politically important organizations are the main target of those insider threats. Organizations often take precautions and measures against the threats of outsides. But the employees, vendors work closely with them. They know the weakness and the network structure of that particular company. They can easily collect information about the network infrastructure, its devices and its vulnerabilities.

Insiders often do abnormal activities to gain access. Based on research covered we can categorize insiders into several types. Different research papers have described the types differently. We have studied them and found out seven types of insider threats with some of them having slightly difference. They are Malicious, Accidental, Career Oriented, Negligent, Oblivious, Mischievous, Emotional.

Malicious insider is who intentionally looks for credentials maliciously to steal information for financial and personal gain. This kind of insider sells information to the competitors. This kind of insider basically has complete knowledge about the security policies and vulnerabilities of the organization [2]. Rogue Admins, Perpetrator, Traitor, Terrorist are groups that can be told as Malicious.

Some times employees mistakenly do some damage to the company network or delete sensitive data, they can be told as Accidental Insider Threats.

There are employees who has high ambitious in their career. They got offers from competitor to remove data or important credential of his/her own company. We can segmented as career oriented.

Negligent insider basically make common types of mistakes and are generally careless about the security policies of that organization. They unknowingly expose the organization's security to the outsiders. Employees click insecure links which may lead to a successful bridge of connection with the attacker.

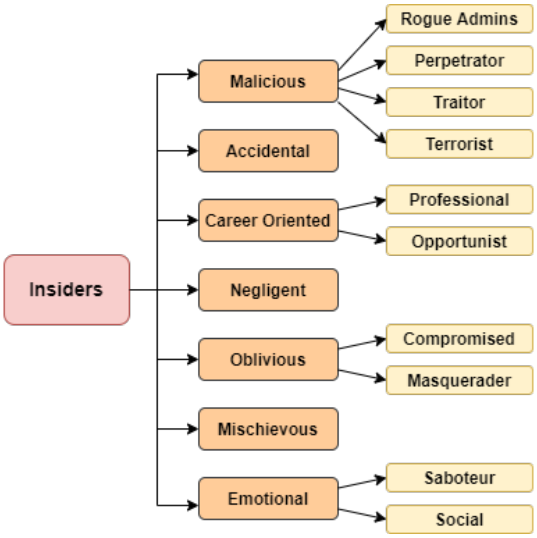


Fig. 1. Different kinds of insider

Oblivious Attacker targets this kind of insider and gains access to the organization's network infrastructure by harvesting his/her login credentials. Social engineering is a technique representing malicious activities that are targeted through human interactions to either inject malware or retrieve sensitive information. It applies psychological manipulation to trap users making security mistakes or overlook associated risks [2]. Detecting this kind of attack is very difficult in a sense that the attacker is using valid credentials to enter the system.

Insider can be harmful to company if they emotionally do some damage. If there are any hard word going on between management and the employees, emotionally vulnerable employees can be turned into insider threats for the company.

Mischievous insiders are the employees who likes to take risk and try new things. For their experiments or trying new things they can be the cause of data ex-filtration.

1) Challenges: After reviewing several research paper we have come out some challenges that needs to address while addressing insider attack: 1) Educate employee to report of suspicious activities 2) Identifying and Monitoring suspicious transaction behavior 3) Measuring deviance in the automated tools We would like to continue the study and find the challenges and will proposed a complete taxonomy.

2) Our Contribution: If organizations want to fight against malicious insiders they need to take both prevention and detection techniques. In this paper a complete review of prevention and detection techniques will be presented. In addition to that the challenges of the detection techniques will also be covered. We will evaluate recent detection techniques used by several organizations. A complete taxonomy on different types of detection, prevention and mitigation techniques will be presented.

II. LITERATURE REVIEW

Cloud computing is an emerging technological function that enables the deployment of computer resources and services in a flexible and dynamic manner. Despite the potential advantages of cloud computing, there are still worries regarding cloud service security and privacy. Because the usage of cloud services has an influence on the security postures of businesses and critical infrastructure, it's necessary to recognize and manage the new dangers and hazards that this new paradigm has presented. Internal risks in cloud computing were the focus of this study's authors, an area that has received little scholarly attention thus far. The authors adopted a broad approach to the problem, differentiating two scenarios: fighting against a malicious insider working for the cloud service, and safeguarding against an insider working for a corporation that decides to outsource some or all of its IT infrastructure to the cloud. To alleviate the situation, possible difficulties for each scenario are identified, and effective remedies are provided. [3]

This [4] study looked at malicious insiders in general and especially with regard to cloud computing. While the existing CERT and RAND definitions are sufficient to safeguard insiders in cloud computing, they fall short of capturing the full scope of the vast and complex idea of cloud computing. It was shown that the line between outsiders and insiders in the cloud ecosystem may be hazy at times, and that there are several additional participants in the cloud ecosystem, including family and friends, acid clouds, nation-states, organized crime, and other cloud customers. Insider assaults in the cloud ecosystem will be difficult to detect in a variety of ways, including through the cloud platform. Customers are usually uninformed about the mechanics of data management. As a consequence, the consumer has no idea where their data is kept or how many copies there are. In many circumstances, the terms of service will permit the usage of third-party organizations that the customer is ignorant of.

The authors discuss the common conception of a cloud insider as a rogue administrator of a service supplier, but they also suggest different other cloud-related insider threats: the insider who uses cloud systems to control an in-house employer's local data sources, and the insider who conducts cloud-based threats for stealing information from a cloud system. They also detailed a cloud service provider's hierarchy of administrators, demonstrated how the nature of cloud system designs allows for successful attacks, and presented real-world examples of insider threat attacks with required and likely responses. [5] Cloud-related insider threats are widely considered a critical issue by cybersecurity professionals, but this danger has not yet been studied in depth. We believe that the fundamental basis of existing insider threats will remain fundamentally unchanged in a cloud computing environment, although this paradigm exposes new options for exploitation. We describe the general concept of a data center insider as a rogue assistant to a service provider, but we also present two other cloud-related insider risks: the insider who exploits a cloud-related vulnerability to steal information from a cloud system and the insider who uses cloud systems to conduct an attack on an employer's local resources. We even describe the hierarchy of administrators at a cloud provider and present real-world cases of insider attacks. [5]

Artificial intelligence (AI) is one of the most dependent on Cloud computing on the other hand, has found several applications and is widely being explored in providing security specifically for IoT devices. Malicious insider attacks are the biggest security challenge related to the IoT devices. Although, most of the analysis in IoT security has pondered on the suggesting of preventing illegal and unauthorized access to systems and information; sadly, the foremost damaging malicious insider attacks that square measure typically a consequence of internal exploitation among Associate in Nursing IoT network remains unaddressed. Therefore, the main target of this analysis is to sight malicious insider attacks within the IoT surroundings mistreatment AI. This analysis presents a light-weight approach for detective work insider attacks and has the potential of detective work anomalies originating from incoming knowledge sensors in resource forced IoT environments. The results and comparison show that the planned approach achieves higher accuracy as compared to the state of the art in terms of: improved attack detection accuracy, minimizing false positives and reducing the computational overhead. [6]

This section proceeds with a security mechanism in the RPL protocol. An intrusion detection system (IDS) will be accustomed to detect attacks on a system. The role of an IDS is to monitor the performance of a laptop or network system and to investigate it for signs of intrusion. In an IDS, 3 main modules of observation, identification, and analysis are used. The primary module observes network traffic and resources. Identification and analysis are the most parts of an IDS that are used to notice intrusion supporting a particular rule. Necessary alerts may well be sent when distinctive network intrusions. IDS will be accustomed to monitor unknown traffic in a chosen node, observe the performance of each network and nodes, and notice each external and insider attack. In general, this is four varieties of IDS: signature-based, anomaly-based, specification-based, and hybrid. Signature-based IDS focuses on distinctive "known attacks," therefore it's additionally referred to as rule-based intrusion detection. This system involves signatures or some predefined patterns that may be held on during an info. Depending on a predefined pattern or individual attack signature, every attack will be known by exploring parameters that are acknowledged during an info for an insider attack. The better-known parameters are the attack signature and, thus, the kind of an IDS. The limitation of this method is that unpredictable attacks on the system can not be detectable. Therefore, it's necessary for the database to be frequently updated with new attack or signature patterns. [7]

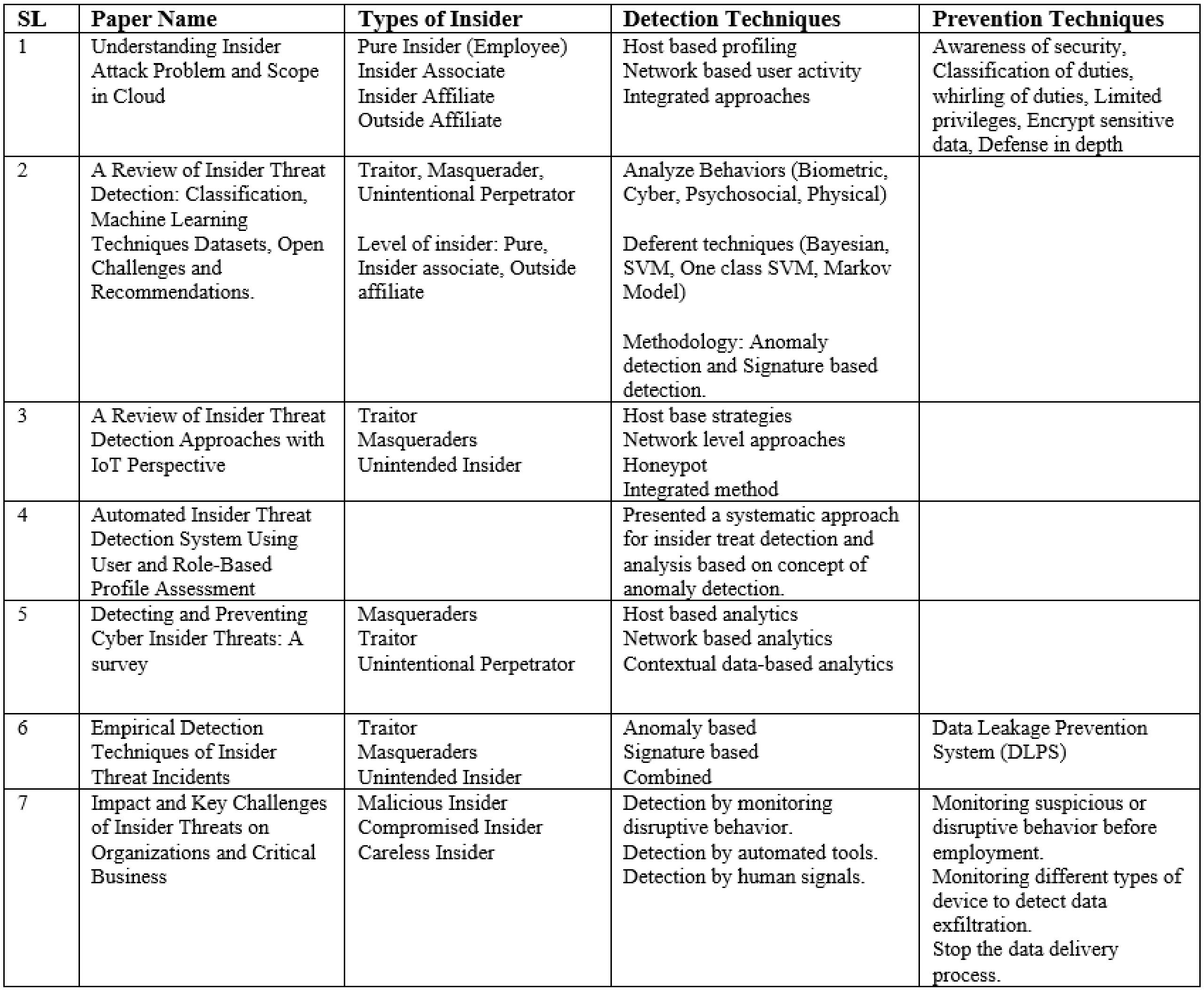
Insider threats are far less common than external network attacks, but can nonetheless do significant damage. Traditional methods for detecting insider threats rely on rule-based approaches developed by domain specialists. Insider-threat detection methods based on user behavior modeling and anomaly detection algorithms are proposed. Anomaly detection can function well for unbalanced datasets with minimal insider threats and no domain experts' knowledge. We created three types of datasets based on user log data: a daily activity summary, email contents subject distribution, and a user's weekly email conversation history. Then, we used four anomaly detection techniques and their combinations. An insider-threat detection system based on anomaly detection techniques and user behavior modeling. Each row is associated with an instance (user-day, email content, user-week). Insider-threat models replicate real-world organizations where just a few insiders' behaviors are potentially harmful. When expanded to include the top 30% of anomaly scores, more than 90 percent of real anomalous behaviors were recognized for two of the three positions studied. The threat detection rate for malicious emails increased dramatically when the top 30% of suspicious emails were monitored. Despite the fact that the CERT dataset was crafted to include a variety of threat scenarios, it is still a simulated and artificially formed dataset. The suggested framework could be further proven if verified using a real-world dataset. [8]

Insiders are suspected in 27 percent of all cybercrime occurrences, and 30 percent believe the damage produced by insiders is more severe than that caused by outside attackers. Insider threats are one of the most difficult assault models to combat just like they are in the real world. In a study of economic crime, internal fraudsters were shown to be the primary culprit in 29% of cases. Only 11% of respondents believed their organization was not vulnerable to insider assaults. 89% said their firm was at least somewhat vulnerable to such assaults. Insiders are authorized users who have legitimate access to sensitive/confidential information. Unintended insider threats have become more common in recent years. There is a lot of motive to deal with insider threats, and it's just going to get stronger. [9]

In [10] author discussed about the prevention and detections techniques. To cope up with insider attack organizations should concern more about their prevention techniques. Before employment they should monitor suspicious or disruptive behavior before employment. Company should check background of the employee and previous employment history. If he/she has any kind of suspicious activity record he/she should not have been recruited. Employees need to use different kind of devices to run office work, they also use personal devices. According to [] Microsoft windows has developed group policies by which admin can control the devices to be installed in the system. There is a system named Virtual Desktop Infrastructure (VDI), in which data stored in a remote server and user interact with locally installed application. This prevents user from initiating data exfiltration. [9] Table I describe briefly represent the above mention prevention techniques.

Detection technique can be segmented by three phases; detection by disruptive behavior, by automated tools, by human signals. The methods of those three types of detection technique has been shown in Table II. In our finding we have also identified the challenges for those detection techniques. [2]

Table I: Detection and Prevention Techniques



SL	Paper Name	Types of Insider	Detection Techniques	Prevention Techniques
1	Understanding Insider Attack Problem and Scope in Cloud	Pure Insider (Employee) Insider Associate Insider Affiliate Outside Affiliate	Host based profiling Network based user activity Integrated approaches	Awareness of security, Classification of duties, whirling of duties, Limited privileges, Encrypt sensitive data, Defense in depth
2	A Review of Insider Threat Detection: Classification, Machine Learning Techniques Datasets, Open Challenges and Recommendations.	Traitor, Masquerader, Unintentional Perpetrator Level of insider: Pure, Insider associate, Outside affiliate	Analyze Behaviors (Biometric, Cyber, Psychosocial, Physical) Deferent techniques (Bayesian, SVM, One class SVM, Markov Model) Methodology: Anomaly detection and Signature based detection.	
3	A Review of Insider Threat Detection Approaches with IoT Perspective	Traitor Masqueraders Unintended Insider	Host base strategies Network level approaches Honeypot Integrated method	
4	Automated Insider Threat Detection System Using User and Role-Based Profile Assessment		Presented a systematic approach for insider treat detection and analysis based on concept of anomaly detection.	
5	Detecting and Preventing Cyber Insider Threats: A survey	Masqueraders Traitor Unintentional Perpetrator	Host based analytics Network based analytics Contextual data-based analytics	
6	Empirical Detection Techniques of Insider Threat Incidents	Traitor Masqueraders Unintended Insider	Anomaly based Signature based Combined	Data Leakage Prevention System (DLPS)
7	Impact and Key Challenges of Insider Threats on Organizations and Critical Business	Malicious Insider Compromised Insider Careless Insider	Detection by monitoring disruptive behavior. Detection by automated tools. Detection by human signals.	Monitoring suspicious or disruptive behavior before employment. Monitoring different types of device to detect data exfiltration. Stop the data delivery process.

III. Methodology

At first, the search keywords were decided on which was used for selecting literature for our review paper. The 'AND' and 'OR' syntax is used while searching. 'AND' here defines the word that was surely used for searching and 'OR' describes any of the words that can be chosen from the selected words. Search keywords are shown in Table 2. And Inclusion and Exclusion Criteria has been discussed in Table 3.

A. Research Questions

i) Is the idea and classification of Insiders are clearly achieved? ii) Can further researchers will get an overall idea of the classification of insiders? iii) Does Insider attacks depend on only technical or hardware/software perspective? iv) How can We use this work for future purposes? v) What Corporate can do to detect, prevent and mitigate insider attacks and how do this? vi) What the motivations, vulnerabilities of insider threats? vii) How can use techniques of insider attack detection and prevention in cloud security?

We have already discussed a comprehensive classification of Insiders. The classification includes malicious, negligent, accidental, oblivious, mischievous, career-oriented, and emotional. We have discussed the insiders' properties in previous sections.

IV. Detection Techniques

1) Honeypot: It is a detection process of cyber security that main system is essentially a parent process with multiple child processes handling individual tasks. Service Log Monitors: These programs are in charge of interpreting service log files. The data from the various service logs is updated in an in-memory cache/standard data pipeline that is shared with the parent process. The system now consists of four service log monitors, each of which is responsible for monitoring exposed services such as SSH, FTP, HTTP, and MySQL.

Table 2: Paper Search Keywords

Serial	Search Keyword
1	“Cloud” AND “Computing”
2	“Attacks” OR “Threats” AND “Cloud”
3	“Insider” AND “Attack”
4	“Insiders” AND “Cloud” AND “Computing”
5	“Malicious Insiders” AND “Attack”
6	“Prevention” AND “Technique” AND “Insider” AND “Attack”
7	“Detection” AND “Insider” AND “Attack” AND “Challenges”

Table 3: Paper Inclusion and Exclusion Criteria

Inclusion Criteria		Exclusion Criteria	
IC1	The studies focused on cloud computing based explanations	EC1	Duplicate articles
IC2	The studies which are based on insider attacks	EC2	Exclude the articles which discuss on attacks but not insider attack
IC3	Language must be English	EC3	Not dedicatedly on cloud computing’s perspective
IC4	The studies must be from after 2000 to present	EC4	Excludes the studies which explains the insider attacks but don’t hold technicality

Table 4: Comparison with other Literatures

Serial	**Reference**	**Year**	**Detection Technique**	**Prevention Technique**	**Challenges**
1	17	2015	Yes	Yes	No
2	19	2020	Yes	No	Yes
3	14	2020	Yes	No	No
4	15	2017	Yes	No	Yes
5	13	2018	Yes	Yes	No
6	11	2020	Yes	Yes	No
7	2	2020	Yes	Yes	Yes
8	20	2018	Yes	Yes	Yes
9	21	2019	Yes	Yes	No
10	22	2011	Yes	Yes	No
11	23	2020	Yes	No	Yes
12	24	2017	No	Yes	Yes
13	25	2018	Yes	No	No
14	26	2016	Yes	No	Yes
15	27	2013	Yes	Yes	Yes
17	28	2017	Yes	No	No
18	29	2017	Yes	No	No
19	30	2015	Yes	No	No
20	33	2016	No	Yes	No
21	Our Paper	2022	Yes	Yes	Yes

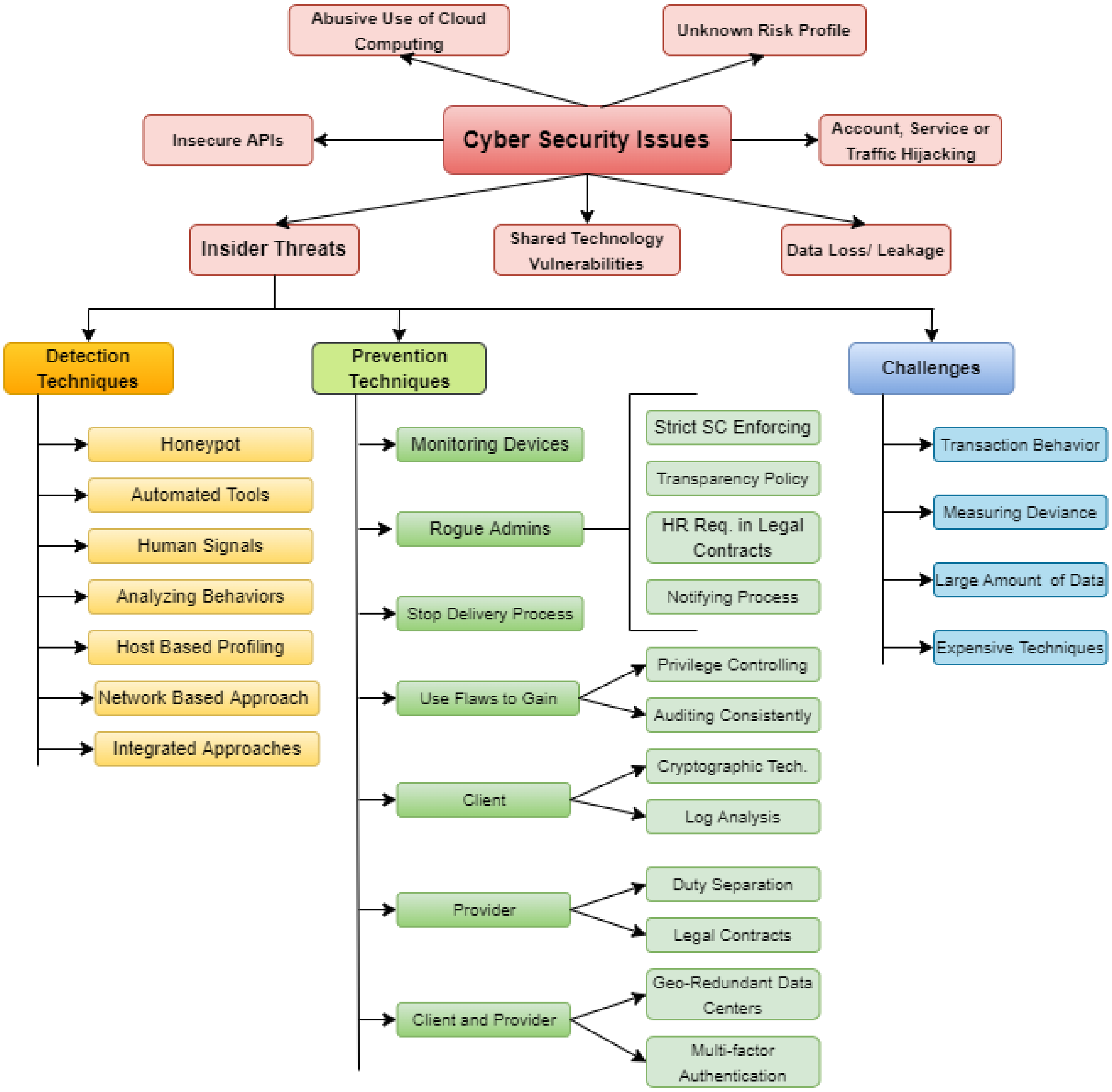


Fig. 2. A Taxonomy on Detection and Prevention Technique of Insider Attack

The parent process manages the Action process, which takes any action depending on the suspicious events reported by the Service Log Monitors. The action is determined by the severity of the malicious events that have been triggered for a specific IP address. Normal, Possible Attackers, Attack pattern discovered, and blocked are the three sorts of activities in the severity table. The system will just allow any additional communication from that particular remote server in the Normal phase. The remote host packet count does not reach the threshold value during the normal phase.

2) Host Based Profiling: Internal events on host machines are analyzed, and behavioral patterns that deviate from normal system and process activity are detected by host intrusion detection systems. Application updates are an important component of observing process behavior since they can affect an application's behavior while also potentially helping to construct a profile for the application by observing its update patterns. During a 100-day investigation period, we observe the update frequency and patterns of a set of programs on 100 machines. Our preliminary findings suggest that unambiguous software update trends can be detected and used to profile operations.

3) Automated Tools: The acronym 'ATR,' which stands for automatic threat recognition or assisted target recognition, is widely used to refer to automatic detection tools. To create such solutions, big data, cloud computing, machine learning, and advanced data analytics have been effortlessly combined.

4) Network Based Approach: Computer networks have given global communication new dimensions. Intrusions and misuses, on the other hand, have always posed a threat to safe data exchange via networks. As a result, network security has become a concern. In today's security infrastructures, intrusion detection systems are critical. Intrusions usually begin with intruders breaking into a network via a vulnerable host and then approaching for further harmful attacks. The intrusion detection techniques employed have their own set of restrictions. Any of the intrusion detection systems that have been proposed thus far are not without flaws. Both host-based and network-based systems have their own set of constraints. As a result, the drive for improvement continues.

5) Human signal: Every employee in a company should be regarded as a member of the detection system. However, in order for this ideology to work, people must first understand what is right and wrong, then know what to report, how to report what they believe is a possible incident, and feel comfortable following through with the complaint. To do this, the security program must develop an environment that encourages the dissemination of required information while also providing the necessary level of comfort. An incident detection algorithm is much stronger when you can establish this type of environment. In addition, the organization's ability to react has improved. This chapter takes readers through the challenges of building an environment in which everyone is enlisted to help with the security program.

6) Behavior Analyzing: To facilitate remote management, monitoring, and reporting, cyber-physical systems (CPS) are frequently network connected. As a result of this integration, they are vulnerable to cyber attacks emanating from an untrustworthy network (e.g., the internet). When a network's security is breached, an attacker risks corrupting the system's functions, which could result in disasters. As a result, detecting intrusions into mission-essential CPS is critical. Signature-based detection may not be suitable for CPS, whose complexity may limit the use of any concise signatures. Due to the CPS's complexity and dynamics, as well as inaccuracies and incompleteness of design documentation or operation manuals, specification-based detection necessitates exact definitions of system behavior, which might be difficult to achieve. Formal models, to be precise.

7) Integrated Approach: The attack detection rate is relatively high; this can be accomplished by combining a layered technique with enhanced fuzzy multi-objective particle swarm optimization, which successfully selects features. The fuzzy based support vector machine approach is useful for detecting anomalous attacks. When compared to previous systems that take a long time to train to detect unknown attacks, the newly presented system is likely to be more efficient in detecting U2R attacks. In addition, our technology detects in a very short amount of time. The proposed system has a detection rate of up to 99.1

V. Prevention Technique

A. Awareness of cyber security

What is the Importance of Cybersecurity Awareness? Cybersecurity events, like other types of incidents, can cost a lot of money. If you're having trouble deciding how much money to spend on cybersecurity training, tools, or talent, consider risk management. With the amount of cyberattacks increasing every year, the risk of not educating your personnel on cybersecurity awareness is only increasing. Cybercriminals are always devising new ways to get around the most up-to-date defensive systems and technologies, landing in your employees' inboxes and browsers. In only 2021, humans were engaged in 85

B. Encryption data

Encryption is a cybersecurity strategy that secures private and confidential data by scrambling it with unique codes that make it impossible for outsiders to read. Encryption ensures that an institution's private data encryption procedure is simple. The plaintext data is translated into unreadable data, also known as ciphertext, using an encryption key and a specific encryption technique. Intruders will not be able to read the data if they get past the system security measures because the jumbled data can only be decoded with the associated encryption key. Secure Sockets Layer (SSL) is a data encryption protocol used by websites to protect sensitive user information. It protects sensitive user data in transit to and from the website from being accessed by intruders. The URLs of websites that have incorporated SSL security feature a padlock icon and use ”https” instead of ”http” for their link address. The usage of SSL ensures that the website's users are protected.

C. Data leakage Prevention

The practice of identifying and preventing data breaches, exfiltration, or unauthorized deletion of sensitive data is known as data loss prevention (DLP). DLP is used by businesses to protect and secure their data while still adhering to rules.

The term ”data leakage prevention” refers to defending companies against both data loss and data leaking. When vital data is lost to the enterprise, such as in a ransomware attack, it is referred to as data loss. The goal of data loss prevention is to prevent data from being transferred outside of a business. DLP is commonly used by businesses to:

Protect Personally Identifiable Information (PII) and follow all applicable laws. It is vital for the organization to protect its intellectual property. In large businesses, achieve data visibility. In BYOD (Bring Your Own Device) situations, secure your mobile workforce and enforce security.

1) Ongoing Attack Monitoring: We look for mitigation controls for 17 different forms of cyber threats, including account compromise, unauthorized access, ransomware, network intrusions, malware infections, sabotage, and security policy violations, among others.

2) Cloud Security Monitoring: Microsoft 365 includes more than 280 security options. Hundreds of security setting options are available in Amazon Web Services and Azure.

D. Prevention Data Exfiltration

Keeping sensitive data inaccessible to unauthorized third parties is an important function of computer and network security. This document examines the features of data exfiltration threats and discusses industry-wide data security best practices. It demonstrates how to leverage Google Cloud's tools and features to mitigate risks, detect data exfiltration, and respond to data exfiltration incidents. Security risks and defense strategies will be described in a cloud-independent environment whenever possible. The changing legal landscape, particularly the European General Data Protection Regulation (GDPR), which takes effect in 2018, has placed a renewed emphasis on the deployment of data exfiltration prevention methods.

E. Protection Against Rogue Administrators

A cloud service provider's malicious administrator Researchers most frequently address this cloud-related insider. Theft of sensitive information, leading to a loss of data confidentiality and/or integrity, is a common assault proposed by this insider. This threat's insider might be motivated by money, which is a frequent incentive for theft of intellectual property or fraud. IT sabotage, on the other hand, is a type of assault in which an employee tries to harm an employer's IT infrastructure i)Strict Supply Chain Enforcing ii)Conducting Supplier Assessment iii)Include Human Resource requirements in legal contracts. iv)Apply transparency policy in overall management practice v)Introduce notifying processes for security breaches

F. Use Flaws to Gain

The insider within the business who exploits vulnerabilities revealed by the usage of cloud services to obtain unauthorized access to organization systems and/or data is the second form of cloud-related insider threat that security researchers generally miss. This might be intentional or unintentional, and it's occasionally made possible by discrepancies in security rules or access control models between cloud-based and local systems. Because direct administrative control of technology and data is difficult for an organization to implement fast, this threat may succeed. i) Diligence and planning in implementation. ii) Maintaining cloud services. iii) Properly maintained responsibilities iv) Privilege Controlling v) Auditing Consistently vi) Taking care of data loss

G. Using the Cloud Services to Initiate Obnoxious Activities

The third form of cloud insider is someone who utilizes cloud services to launch a cyberattack on his own company. This is comparable to the previous sort of insider, which targets cloud-based systems or data. The third sort of insider, on the other hand, uses the cloud as a tool to carry out attacks on systems or data that aren't necessarily affiliated with cloud-based services.

1) Protections/Solution: Using data loss prevention tools can be effective for the detection of sensitive data being sent via email or uploaded to storage. Limit employee access to resources under host-based controls.

Existing data protection techniques, such as encryption, have proven ineffective in stopping data theft attempts, particularly those carried out by a cloud provider's insider. They recommended employing offensive decoy technology to secure data in the cloud in a novel way. They kept track of data access in the cloud and identified any unusual tendencies. They started a misinformation assault by returning significant volumes of decoy material to the attacker when illegal access is detected and then validated using challenge questions. This prevents the user's personal information from being misused. Experiments in a local file setting show that this method might give unparalleled levels of user data protection in a Cloud context.

These threats can be minimized by cloud developers through the deployment of identity and access management (IAM) technologies and two-factor authentication. Checking the background and monitoring the behavior of privileged employees is essential to reduce malicious activities of insiders. Security breach notification system to be implemented.

VI. Our Future work Plan

Traditionally, a large number of malicious insiders were motivated by petty motives such as vengeance, work conflict, and entitlement. This is still true today. Profit, outside influence, and ideology are now becoming more important factors, leading to longer, more sustained, and more untactful insider attacks. i) Easier Attack Vector ii) Digital Black Markets iii) Remote Employment Vulnerabilities iv) Modern technology use v) Increase Privilege escalation vi) Data Transfers Security improve with data ex filtration

VII. Conclusion

Our paper which focuses on the detection and prevention of insider attacks, demonstrates that the Work from Home movement has revealed a blind spot in visibility to employee behavior. The potential of insider trading is a serious concern for all corporation. A recurring research difficulty has been developing an effective mitigation technique to fight the issue. Security has prioritized external threats while treating insiders as trusted simply because they are on the corporate network. Organizations must be alert to suspicious and malicious activities, particularly those occurring within the insider threat kill chain. At the same time, workforce cyber intelligence efforts must not be interpreted as employee spying or an unfounded lack of trust. Traditional cyber security and workforce monitoring tools lack the context and abnormal behavior insight needed to detect malicious activity. Moreover, they lack the ability to do so while also fostering a culture of trust. We have explained, reviewed, and discovered some detection and prevention techniques based on our taxonomy to protect against insider threats and how organizations can protect their sensitive data and the privacy of their workforce.

References

[1] J. Joshi, "Insider Threats: Challenges and Mitigation Approaches."

[2] N. Saxena, E. Hayes, E. Bertino, P. Ojo, K. K. R. Choo, and P. Burnap, "Impact and key challenges of insider threats on organizations and critical businesses," Electronics (Switzerland), vol. 9, no. 9. MDPI AG, pp. 1–29, Sep. 01, 2020. doi: 10.3390/electronics9091460.

[3] A. Duncan, S. Creese, M. Goldsmith, and J. S. Quinton, "Cloud computing: Insider attacks on virtual machines during migration," in Proceedings - 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2013, 2013, pp. 493–500. doi: 10.1109/TrustCom.2013.62..

[4] A. J. Duncan, S. Creese, and M. Goldsmith, “Insider attacks in cloud computing,” in Proc. of the 11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012 - 11th IEEE Int. Conference on Ubiquitous Computing and Communications, IUCC-2012, 2012, pp. 857–862. doi: 10.1109/TrustCom.2012.188.

[5] W. R. Claycomb CERT R and A. R. Nicoll CERT, “Insider Threats to Cloud Computing: Directions for New Research Challenges.”

[6] A. Y. Khan, R. Latif, S. Latif, S. Tahir, G. Batool, and T. Saba, “Malicious Insider Attack Detection in IoTs Using Data Analytics,” IEEE Access, vol. 8, pp. 11743–11753, 2020, doi: 10.1109/ACCESS.2019.2959047.

[7] N. Jahantigh and A. B. Shahri, “Intrusion Detection System to Detect Insider Attack on RPL Routing Protocol Based on Destination Advertisement Object.”

[8] J. Kim, M. Park, H. Kim, S. Cho, and P. Kang, “Insider threat detection based on user behavior modeling and anomaly detection algorithms,” Applied Sciences (Switzerland), vol. 9, no. 19, Oct. 2019, doi: 10.3390/app9194018.

[9] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici, and M. Ochoa, “Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures,” ACM Computing Surveys, vol. 52, no. 2. Association for Computing Machinery, May 01, 2019. doi: 10.1145/3303771.

[10] S. Prabhu and N. Thompson, “A Unified Classification Model of Insider Threats to Information Security.” [Online]. Available: https://www.researchgate.net/publication/348129016

[11] R. A. Alsowail and T. Al-Shehari, “Empirical detection techniques of insider threat incidents,” IEEE Access, vol. 8, pp. 78385–78402, 2020, doi: 10.1109/ACCESS.2020.2989739.

[12] S. O. Kuyoro, A. Oludele, and K. S. O, “View project,” 2011. [Online]. Available: https://www.researchgate.net/publication/285011991

[13] L. Liu, O. de Vel, Q. L. Han, J. Zhang, and Y. Xiang, “Detecting and Preventing Cyber Insider Threats: A Survey,” IEEE Communications Surveys and Tutorials, vol. 20, no. 2. Institute of Electrical and Electronics Engineers Inc., pp. 1397–1418, Apr. 01, 2018. doi: 10.1109/COMST.2018.2800740.

[14] A. Kim, J. Oh, J. Ryu, and K. Lee, “A review of insider threat detection approaches with IoT perspective,” IEEE Access, vol. 8, pp. 78847–78867, 2020, doi: 10.1109/ACCESS.2020.2990195.

[15] P. A. Legg, O. Buckley, M. Goldsmith, and S. Creese, “Automated Insider Threat Detection System Using User and Role-Based Profile Assessment,” IEEE Systems Journal, vol. 11, no. 2, pp. 503–512, Jun. 2017, doi: 10.1109/JSYST.2015.2438442.

[16] “Insider Threat Detection: A Solution in Search of a Problem,” 2020.

[17] T. Gunasekhar, K. T. Rao, and M. T. Basu, “Understanding insider attack problem and scope in cloud,” Jul. 2015. doi: 10.1109/ICPCT.2015.7159380.

[18] Institute of Electrical and Electronics Engineers, 2020 IEEE Conference on Communications and Network Security (CNS).

[19] L. Liu, O. De Vel, Q. L. Han, J. Zhang and Y. Xiang, ”Detecting and Preventing Cyber Insider Threats: A Survey,” in IEEE Communications Surveys Tutorials, vol. 20, no. 2, pp. 1397-1417, Second quarter 2018, doi: 10.1109/COMST.2018.2800740.

[20] Ivan Homoliak, Flavio Toffalini, Juan Guarnizo, Yuval Elovici, and Martín Ochoa. 2019. Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. ACM Comput. Surv. 52, 2, Article 30 (March 2020), 40 pages. https://doi.org/10.1145/3303771

[21] Y. Chen and B. Malin, “Detection of anomalous insiders in collaborative environments via relational analysis of access logs,” in Proc. 1st ACM Conf. Data Appl. Secur. Privacy (CODASPY). New York, NY, USA: ACM, 2011, pp. 63-74

[22] A. Y. Khan, R. Latif, S. Latif, S. Tahir, G. Batool, and T. Saba, ‘Malicious insider attack detection in IoTs using data analytics,” IEEE Access, vol. 8, pp. 11743-11753, 2020.

[23] A. Almehmadi and K. El-Khatib, “On the possibility of insider threat prevention using intent-based access control (IBAC),” IEEE Syst. J., vol. 11, no. 2, pp. 373-384, Jun. 2017.

[24] P. Chattopadhyay, L.Wang, and Y.-P. Tan, “Scenario-based insider threat detection from cyber activities,” IEEE Trans. Comput. Social Syst., vol. 5, no. 3, pp. 660-675, Sep. 2018.

[25] I. A. Gheyas and A. E. Abdallah, “Detection and prediction of insider threats to cyber security: A systematic literature review and metaanalysis,”Big Data Analytics, vol. 1, no. 1, p. 6, Dec. 2016.

[26] D. Kim and M. G. Solomon, Fundamentals of information systems security. Jones Bartlett Learning, 2016

[27] G. J. Silowash and C. King, “Insider threat control: Understanding data loss prevention (dlp) and detection by correlating events from multiple sources,” DTIC Document, Tech. Rep., 2013

[28] A. Gamachchi, L. Sun, and S. Boztas, “Graph based framework for malicious insider threat detection,” in Proceedings of the 50th Hawaii International Conference on System Sciences, 2017

[29] A. Tuor, S. Kaplan, B. Hutchinson, N. Nichols, and S. Robinson, “Deep learning for unsupervised insider threat detection in structured cybersecurity data streams,” in AI for Cybersecurity Workshop at AAAI, 2017

[30] M. Eikel and C. Scheideler, “Iris: A robust information system against insider dos attacks,” ACM Transactions on Parallel Computing, vol. 2, no. 3, p. 18, 2015

[31] G. J. Silowash and C. King, “Insider threat control: Understanding data loss prevention (dlp) and detection by correlating events from multiple sources,” DTIC Document, Tech. Rep., 2013

[32] N. T. Nguyen, P. L. Reiher, and G. H. Kuenning, “Detecting insider threats by monitoring system call activity,” in IAW. Citeseer, 2003, pp. 45–52

[33] K. Bhavsar and B. H. Trivedi, “An insider cyber threat prediction mechanism based on behavioral analysis,” in Proceedings of International Conference on ICT for Sustainable Development. Springer, 2016, pp. 345–353

[34] W. T. Young, H. G. Goldberg, A. Memory, J. F. Sartain, and T. E. Senator,“Use of domain knowledge to detect insider threats in computer activities,” in Security and Privacy Workshops (SPW). IEEE, 2013, pp. 60–67.

[35] Y. Liu, C. Corbett, K. Chiang, R. Archibald, B. Mukherjee, and D. Ghosal, “Sidd: A framework for detecting sensitive data exfiltration by an insider attack,” in System Sciences. IEEE, 2009, pp. 1–10

[36] J. Hunker and C. W. Probst, “Insiders and insider threats-an overview of definitions and mitigation techniques.” JoWUA, vol. 2, no. 1, pp. 4–27, 2011.