

# A systematic literature review on insider threats

Angad Pal Singh  
School of Engineering  
University of Guelph  
Guelph, Canada  
angadpal@uoguelph.ca

Ankit Sharma  
School of Engineering  
University of Guelph  
Guelph, Canada  
asharm50@uoguelph.ca

**Abstract**—Insider threats is the most concerned cybersecurity problem which is poorly addressed by widely used security solutions. Despite the fact that there have been several scientific publications in this area, but from our innovative study classification and structural taxonomy proposals, we argue to provide the more information about insider threats and defense measures used to counter them. While adopting the current grounded theory method for a thorough literature evaluation, our categorization's goal is to organize knowledge in insider threat research. Along with an analysis of major recent studies on detecting insider threats, the major goal of the study is to develop a classification of current types of insiders, levels of access, motivations behind it, insider profiling, security properties, and methods they use to attack. This includes use of machine learning algorithm, behavior analysis, methods of detection and evaluation. Moreover, actual incidents related to insider attacks have also been analyzed

**Key Words:** insider threats, security solutions, defense measures, machine-learning, datasets, detection methodologies, evaluation metrics.

## I. INTRODUCTION

Today's digital economy depends on strong cyber security. As opposed to external threats, internal threats to security are the biggest. Important mitigating approaches include the detection and forecasting of insider threats [1]. In the digital era in which we live has both its benefits and drawbacks, just like anything else. The biggest drawback is the security risk. Data breaches are becoming more frequent and important as our sensitive information migrates more toward the digital domain. A case in point would be businesses may be exposed to security hazards from both internal and external sources. For instance, internal attacks are more dangerous than external ones, whether they originate from employees, vendors, or other companies due to having a direct relationship and access to a company's computer system [2]. Because they are familiar with how the organization functions on a daily basis, these insiders have access to all the privileges and permissions necessary to start an attack that is not available to outsiders.

Insiders are able to pass off their attacks as normal operations which makes it difficult to distinguish them [3], [4]. A countermeasure of creating automated threat detection systems that don't raise too many false alarms is the issue at hand. Employees might not be able to access the system during a time-sensitive situation and carry out their tasks successfully in emergency-like situations. In such situations, companies can

become paralyzed by the loss of system availability, which can increase expenses, reduce income and pose real-life threats. One of the most recent case examples to share would be the one where 27,000 of client records were exposed by Barclays bank claimed by a whistleblower employee [5]. Not only did the leak result in loss of trust of the customers, but also resulted in £7.7 million in penalties and ordered to pay impacted parties up to £59 million in compensation. This is one of many incidents that occurred due to insider threats and it is of paramount importance to explore methods to prevent them from happening in today's world [6], [7].

### 1.1. Prior research

To our knowledge, there appears to be very little systematic literature review(SLR), particularly with relation to insider threats in the modern world. One of the latest investigative papers in the field of cyber security and insider threats was by Al-Mhiqani, Mohammed and Ahmad, and various another writer in 2020 [8]. In this study, the authors highlight classification of contemporary insider types, access rights, levels, motives, insider profiles, security properties of validity and methods used by attackers. He also evaluated recent notable research on insider threat detection, including behavior modeling, and used implementing of machine learning algorithms. Several real cases of insider threats were analyzed to provide statistical information on insiders. Additionally, this survey highlights challenges other researchers face and makes recommendations to reduce barriers.

This section discusses insider threat investigations and review articles. Only a handful of documents were found, i.e., Walker-Roberts [9] published a review in 2018. He published a review paper on detecting insider threats; however, the scope of the paper was restricted to medical science. Another review by Ullah [10] was published in 2018 identified and critically analyzed data intrusion attack vectors and countermeasures to report on the state of the art and identify vulnerabilities for future research. In 2011, famous Researchers Hunker and others summarized the main properties related to insiders and threats they cause to organization. [3]. The primary contributions of this review and how it differs from earlier studies can be summed up as follows:. First, to our knowledge, this is the first paper in which we have reviewed numerous papers related to insider threat and summarized a systematic report at the end of the study. Secondly, many incidents related to insiders has also been summarized and discussed. Moreover

a summary and future work recommendation is also provided at the end of the paper. [11].

### 1.2. Research goals

The main goal of this paper is to systematically review the available research papers and to analyze the Insider threat problem. This study addresses the following research questions that has been mentioned in Table I.

### 1.3. Contributions and layout

This SLR is addition to existing study and discuss the following contributions for those with an interest in the field of Cyber Security and threats to further their work:

TABLE I  
RESEARCH QUESTIONS

Research Questions (RQ)	Discussion
RQ1. What is the magnitude and impact of insider threats to businesses globally?	Insider threats has been increased since the introduction of internet, recent survey shows that insider attack increased from 30 % to 51% in couple of years.
RQ2. The common techniques used to carry out insider threats and override controls that are set to detect insider threats in the first place.	The most common insider threats are caused by ex-employee or humans, so to mitigate this companies have adopted policy of changing or revising their system after few years.
RQ3. What methods and techniques are available to overcome and insider threats in the world of cyber security?	Educating our users and strong authentications are the main key methods to overcome this problem.

- We found 50 major studies on insider attacks and cyber security up to 2020. If other researchers desire to continue their work in this particular field, they are welcome to use our list of studies.

- After that, we chose 37 primary studies that meet to the standards we established for quality evaluation. These studies can be used as helpful comparison points for other related research.

- Following that, we made the decision to perform a thorough analysis of the data found in the subset of 37 studies. We then provided the data to illustrate the research idea related to the Threat Detection and it's implementation in cyber world.

- We presented a conclusion at the end after analysis of all the studies.

- We issue a statement and create guidelines for further support work in this area.

This essay is organised as follows: The techniques used to carefully choose the primary studies for analysis are described in the Section II The conclusions of each of the chosen primary research are presented in Section III. The findings in relation to the earlier posed study topics are discussed in Section IV. Section V concludes the and makes some recommendations for more future work.

## II. RESEARCH METHODOLOGY

Our study's objective is to conduct a thorough analysis of the existing literature and analyze insider threats from the perspectives of specialists in the field of cyber security. The purpose of the research questions set above will pave the direction for which the systematic literature review will be carried out. Additionally, the research questions will also limit the scope of the study to prioritize literature to publications

that were published recently as the world of cyber security is ever-revolving. Apart from the number of studies that will be researched and studied on, case examples relating to insider threats will also be shown to examine how insider threats are able to impact the daily lives of individuals. This correlation will better put things into perspective to highlight the importance of insider threats. At present, the literature review stage, our goal is to identify suitable literature to carry out an in-depth investigation to the topics and evaluate whether the research topics will be required to be further redefined or not.

### 2.1. Selection of primary studies

Primary studies were conducted by passing keywords to the search facility or search engine. The Boolean AND and OR were used to conduct the search. The search terms were: ("All Metadata": "Insider Threats" OR "All Metadata": "Insider Threat detection" OR "All Metadata": "computer threats") AND "All Metadata": "security"

("All Metadata": "Insider Threats" OR "All Metadata": "Insider Threat detection" OR "All Metadata": "Computer threats") AND ("All Metadata": "cyber security" OR "All Metadata": "cybersecurity" OR "All Metadata": "cyber-security")

The platforms searched were: - IEEE Xplore Digital Library - ScienceDirect - SpringerLink - ACM Digital Library - Google Scholar

Deep research was performed on titles, keywords or summaries, depending on the search platform. On October 9, 2022 We started looking for papers and we processed all studies published up to that date. The results of these searches are filtered using inclusion/exclusion criteria. At the end Snowball iteration forward and backward is performed to filter the papers. Only those papers are selected that meet the inclusion criteria.

### 2.2. Inclusion and exclusion criteria

The research work chosen for this SLR should be only focused on insider threats, it's detection and different techniques used to minimized or lower these attacks on the computer systems. Google Scholar, ACM Library, IEEE platform were searched to narrow down the papers. Those related to insider threats and detections were selected. The inclusion and exclusion criteria are shown in Table II.

### 2.3. Selection results

There was a total of 1323 studies identified by the initial keyword searches on the chosen platforms. After eliminating the duplicate research, this number was drastically reduced to 567. The research that met the inclusion/exclusion criteria were thoroughly examined, and 177 publications were left over for reading. Only papers written in English and published before 2020 were chosen. After reading all 177 papers in detail and using the inclusion/exclusion criteria once again, 50 papers were left for the SLR in the end.

### 2.4. Quality assessment

For the next step Five papers were selected randomly and were subjected to the following quality assessment process to check their effectiveness:

TABLE II  
INCLUSION AND EXCLUSION CRITERIA FOR THE PRIMARY STUDIES.

Inclusion Criteria	Exclusion criteria
The paper should focus on the insider threats and its types	The papers should not be about types of threats, it should focus only on insider threats to the cyber world.
The paper should highlight the insider detection techniques.	Papers published after 2020
The paper should focus on insider threats challenges and its prevention	The paper should focus on insider threats challenges and its prevention.

Stage 1: **Insider Threats:** The paper must be focused on the detection of insider threats and its prevention

Stage 2: **Context:** Adequate context for the research goal and results should be provided. This will allow for accurate study interpretation.

Stage 3: **Insider threats detection:** The study must have sufficient data to accurately depict how the technology was used to solve a particular issue. which will eventually help in solving problem, RQ1 and RQ2.

Stage 4: **Security context:** The paper must provide an explanation for security and privacy concern to answer the problem, RQ3.

Stage 5: **Performance:** The paper should provide enough evidence about performance of the system if the insider threat techniques are applied.

Stage 6: **Data acquisition:** Details about data collection, storing and filtering should be provided to assess how accurate it is.

All identified primary studies were then subjected to this checklist for quality assessment. Thirteen studies were found not to meet the one of the following checklists. So, they were removed from the list as shown in Table III

TABLE III

Checklist for the Criteria Stages	Excluded Studies
Stage 1: Insider Threats	[S47] , [S46] , [S50]
Stage 2: Context	[S42] , [S45]
Stage 3: Insider threats detection	[S39] , [S41], [S44]
Stage 4: Security context	[S43]
Stage 5: Performance	[S40] , [S48] , [S49]
Stage 6: Data acquisition	[S38]

## 2.5. Data extraction

Data were then extracted from all the articles that passed the quality assessment to assess the completeness of the data and verify the accuracy of the information contained in the articles. Before being deployed to all searches that passed the quality review stage, the data mining technique was first tested on years of preliminary investigations. Data from each of the study was extracted, classified into categories, and then entered into a excel sheet. The following categories were applied to the data:

**Context data:** Information on the study's purpose.

**Qualitative data:** The authors' findings and conclusions.

**Quantitative data:** Data obtained when we applied it to study and experiment.

## 2.6. Data Analysis

Data corresponding to the qualitative and quantitative categories was assembled in order to answer all the research questions. The papers filtered after the completion of the data extraction process, were then passed through a meta-analysis process

Figure 1 shows the number of papers selected as the initial result and it also represents the process before selecting the number of final papers.

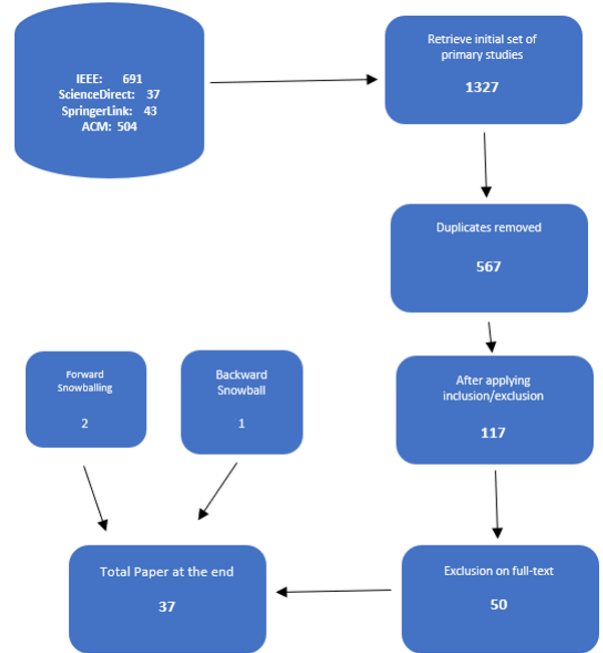


Fig. 1. Attrition of papers through processing.

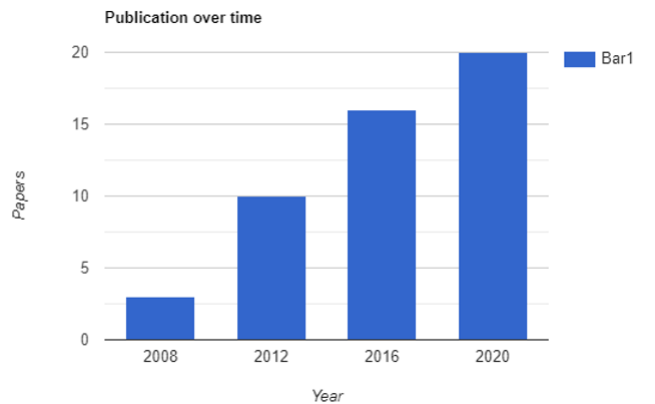


Fig. 2. Number of primary studies published over time

1. Publications over time: As it is clear from the graph in Figure 2 that in recent years, there has been significant

increase in the Publication of papers based on cyber security and insider threats. This is because recent many attacks related to this insider techniques have been occurred globally. This shows that with modernization of internet, increase in threats and cyber security has also boomed in the global market.

2. Significant Keyword Count: An analysis of keywords was performed across all 37 studies in order to summaries the common themes among the selected primary studies. Table IV shows how many times certain words appeared in all of the primary studies. As shown "Insider Attack" is the most frequently occurring keyword in our dataset, following "network" and " Threats" [12], [13].

TABLE IV

Keywords	Count
Insider Attack	1521
Network	1201
Threats	855
Machine Learning	724
National security	356
Humans	250
Cyber	235
Internet	183

### III. FINDINGS

Each primary research study was read thoroughly and relevant qualitative and quantitative information was taken out and summarised in Table V. All the papers has basic information about threat types and its detection. The main theme of paper is also summarized at the end. Each paper was subdivided into broader categories. It is clear from Fig 3, that majority of studies were focused on threat detection and threat mitigation in insider threats. Fig 3, shows the graphical representation of subdivided categories and their applications in insider threats. The themes found in primary studies shows that threat detection and threat mitigation are the most popular security application in insider threats, with both comprising of 35 percent each respectively. These two applications comprise the majority of the studies section. Threat detection discuss about, the detection techniques adopted by companies to track insider threats. Whereas, threat mitigation refers to elimination of the causes of threats in a security system. The third most popular among the primary studies was, modeling human behaviors to detect the insider threat attack (behavior model). It comprises of 19 Percent of the total studies. At the last comes the types of threat, which makes up 11 Percent of the total studies.

### IV. DISCUSSION

Initial keyword searches reveal that there are a large number of papers on Insider Attack. This is due to reason that with advancement in internet more and more social media interaction is causing these attacks. As people are easily convinced on SM and they reveal their secrets to others people and company.

Wide range of papers discuss the threat detection and its removal techniques. insiders are familiar with an

TABLE V  
MAIN FINDINGS AND THEMES OF THE PRIMARY STUDIES.

Primary Study	Key Qualitative and Quantitative Data Reported	Types of Security Applications
[S1]	The author focuses on the insider threats and defense measures against them. They used top 100 papers and identified five different defense solution approaches.	Threat Detection
[S2]	This paper mentions insider threats detection using behavior modeling and algorithms. The author uses log-based data like, browser history, email contacts to detect the insider threats.	Behavior Model
[S3]	Use of machine learning algorithms and mechanism was suggested in this study by the authors. The authors divided the insider behaviors into four different classes and suggested to research more on each indivial class with help of machine learning algorithms.	Behavior Model
[S4]	The paper discusses on how Insider Threats has impacted our critical infrastructure like healthcare and the effectiveness of current defensive measures.	Threat mitigation
[S5]	The author describes the insider attacks and data exfiltration. This study highlights, survey on the data leakage patterns and countermeasures regarding it moreover, author also mentions the three different data states and how often they are attacked.	Threat Type
[S6]	Cyber-attacks have been a main cause of concerns for companies over years. But majority of them are done by the insiders. Author has defined different types of insiders and attacks technique used by them to carry these malicious activities.	Threat Type
[S7]	SCADA systems are prominent in critical infrastructures and preventing them from cyber-attack is important issue. It reviews the current strategies like honey pots used in SCADA and their efficiency.	Threat mitigation
[S8]	With advancement of technology, insider attacks are also becoming advanced. This study investigates different types of risk perception models and its characteristics. A fair solution has been proposed by the author at the end of this study.	Behavior Model
[S9]	This article reviews the involvement of humans in insider attack, and how it really affects the other employees in the group. The author defines how it can trigger the shift in trustworthiness within fellow group member or within the company.	Behavior Model
[S10]	The author explains a famous method known as DLPS (data leakage prevention system) and how it is being utilized by IT companies to protect data breach and leakage. DLPS use different methods to prevent the data leak and author has described its weakness as well as methods to improve them.	Threat Mitigation
[S11]	Here, author describes the newer concept known as Information Security (InfoSec) research, i.e., approaches to prevent intrusion in company system. The study concludes the approaches to detect and mitigate threats using InfoSec.	Behavior Model
[S12]	In this paper, author introduced a new and more efficient way of dealing with insiders. Author divided the threats into two main parts; intentional and accidental. Author suggested to use a new evaluation method based on the profile and position of the users in the system or organization to predict the threats.	Threat Mitigation
[S13]	In this author reviews insider behavior and their role in harming data, whether it's on organization level or cloud level. Author discusses its impact and benefits insider gets from it.	Threat Mitigation

TABLE V  
CONTINUED

Primary Study	Key Qualitative and Quantitative Data Reported	Types of Security Applications
[S14]	Author suggested that single authentication is not efficient method for security. So, the study proposed a new re-authentication method using ensemble technique. Where, author uses keystroke methods to record a pattern to verify the user is authentic or not.	Threat Mitigation
[S15]	In most organization, most of attacks are done by insiders and which are hard to detect. Author defined a system known as Internal Intrusion Detection and Protection System (IIDPS), where system-call patterns were used to record log data and a profile is created according to that.	Behavior Model
[S16]	In This article, author presents an innovative detection method that is robust against mimicry-based evasion strategies. The author divided processing of information into two different stages. First one is analysis stage, where user actions are recorded and then in second stage they are verified.	Threat Detection
[S17]	Author defined that using single model methods to detect insider attacks is not efficient. Study shows that using ensemble technique to detect the threats is better than single model. The author used both of the supervised and unsupervised learning techniques to detect the insider. It came out that supervised learning is better than unsupervised learning.	Threat mitigation
[S18]	This survey paper mentions the SCADA system Vulnerabilities and technique named alarm-and-trust-based access management system (ATAMS). ATAM detect user performance periodically and keeps an eye if an anomaly is detected.	Threat Detection
[S19]	This paper continues the discussion of the risks posed by Hardware like USB devices. Hardware trojan concept is used by author to filtrate data from USB hardware.	Threat Detection
[S20]	This paper mentions the forensic investigation technique to prevent threat attacks. This technique has two phases: first phase is monitoring incoming and outgoing packets and data they contain. Where as in phase two: critical log data is verified for any sensitive information.	Threat Mitigation
[S21]	Because insiders of a company have access to sensitive information, insider attacks can be devastating. This article proposes a novel insider attack authentication protocol based on the dependable cryptographic algorithm known as ECC. It demonstrates that the protocol has a high level of security while being relatively better than other existing protocols in terms of computational cost and communication overhead.	Threat Detection
[S23]	Collaborative intrusion detection networks (CIDNs), allows an IDS to gather data and pick up expertise from others. it has been created to improve the detection accuracy in order to fight against complicated attacks. However, these networks are prone to security issues. therefore, author created an intrusion sensitivity-based trust management model that enables each IDS to assess the trustworthiness of others by checking their detection sensitivity. Author used trust model in a real wireless sensor network and compared the effectiveness of three different supervised classifiers under attack conditions.	Threat Detection
[S24]	The Internet of Things (IoT) is a new approach in computer networks that uses various technologies to connect different objects all around us to each other and Internet. The author introduced a new model for IOT that provides with intrusion detection agents based on both supervised and unsupervised learning and has ability to detect both internal and external attacks simultaneously.	Threat Detection

TABLE V  
CONTINUED

Primary Study	Key Qualitative and Quantitative Data Reported	Types of Security Applications
[S24]	During data transfer, there are two types of data loss. One is link error and another is malicious packet drop. Data lost by malicious activity is always overlooked by researchers. In this paper, author has deeply mentioned and studied the packet drop by malicious activities. Author developed a homomorphic linear authenticator (HLA) based public auditing architecture that verifies the truthfulness of packet loss.	Behavior Model
[S25]	In order to support a conventional type of trust evaluation that includes evidence summing, Author suggest two workable techniques to protect the privacy of trust evidence providers based on additive homomorphic encryption. The first scheme achieves superior computational efficiency. While the second approach offers stronger security.	Threat Mitigation
[S26]	This paper offers a defensive deception strategy that is OS-resident and can be used to neutralize malware infected machine.	Threat Detection
[S27]	One of the main obstacles to the successful implementation of fog computing and the Internet of Things (IoT) is device security. Author described, a three technologies strategy that includes a Markov model, an intrusion detection system (IDS), and a virtual honeypot device (VHD) to recognize malicious devices with the help of fog computing environment	Threat Detection
[S28]	The Article explains the fundamentals of the fog computing technology system, outlines three security issues—creation and use of dummy documents, unidirectional transparent detection—and suggests solutions.	Threat Detection
[S29]	In this study, Author suggested a smart reaction mechanism that constantly manages the operational risks to human operators. Additionally, the architecture of this mechanism enables the system to assume control when areas are completely unprotected and/or isolated in addition to allowing the system to analyses the status of a particular scenario on its own.	Threat Mitigation
[S30]	The author discusses an architecture for overlay networking that is based on gossip protocols, which enable users to communicate with one another other in a safer way. A characteristic of the design is that it limits the quality and quantity of information that insiders may access while optimizing the routing of requests to only include individuals who can respond to them.	Threat Mitigation
[S31]	Author developed a management protocol that prevents both outsider and insider security attacks for group communication systems (GCSs) in mobile ad hoc networks (MANETs).	Threat Mitigation
[S32]	In this study, Author created a software package that could be set up as a gateway between users and the legacy servers. This software uses TCP tunnelling and a hardware device that was scaled down to detect insider attacks.	Threat Type
[S33]	The author mentions, framework based on process models for real-time log data analysis as it is impossible for human auditors to track it.	Threat Detection
[S34]	The primary objectives of this work are to identify and forecast assaults and harmful behaviors through the analysis, classification, and labelling of activities that have been recorded in log files. In this study, each user's behavior is predicted using MapReduce programming. Unknown events are clustered using the K-Means approach, and unlabeled classes are defined using K-NN supervised learning on the NSLKDD database.	Threat Type
[S35]	Author described an approach that can be applied to the challenge of detecting insider threats, specifically the exploitation of an organization's resources by system users.	Threat Detection
[S36]	Author described application of machine learning in Threats. Author used CERT Insider Threat Dataset and applied ML algorithm on them to calculate the results.	Threat Mitigation
[S37]	In this study, Author introduced the community anomaly detection system (CADS), a framework for unsupervised learning that uses access logs from collaborative environments to identify insider threats.	Threat Detection

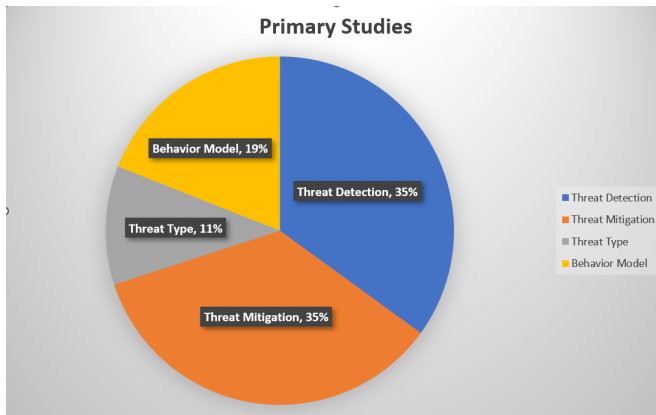


Fig. 3. Chart of themes of primary studies

organization's systems; their malicious behavior is impossible to detect. Therefore [S2], offer a unique way of detecting and minimizing it. The author, proposes an insider threat detection method based on user behavior modeling. The user's daily activity, the delivery of email content topics, and the user's weekly email communication history comprises of common log activities used for detection. As mentioned earlier, in order to protect insider attacks, user behavior as well as hackers' behavior should also be kept in mind [S11]. Every corporation, regardless of size, requires safe IT. Log management is always the critical step while managing firewalls. Article [S33] and [S34] describes how real-time log data analysis is important and how it can be tracked. The log files that are kept on servers, firewalls, and other IT hardware serve as a record of significant transactions and events. This data may offer crucial hints about malicious behavior affecting your network both inside and externally. The analysis of log data can also help in locating and resolving hardware failures as well as setup issues with equipment. Many researchers are shifting their approaches toward the use of Machine Learning for threat Management. In [S35] researchers used CERT Insider Threat Dataset and applied ML algorithm on them. The authors of this study develop a framework called RADISH in and proved that it is capable of detecting insiders using both -Nearest Neighbor (-NN) and -Dimensional Tree (- tree) against the CERT r2 dataset. According to their findings, -NN is often quicker and more accurate than -d tree. Due to this, primary studies have shown rising trend of use of Machine learning in Insider attack detection. Moreover, most of the study pointed that behavior modeling should also be considered. This includes insiders' behavior also, as most the organization neglect their behavior and end up losing data and resources.

#### **RQ 1: What is the magnitude and impact of insider threats to businesses globally?**

It is common that, when a person thinks of insider threats, disgruntled and unethical employee comes in our mind. However, there is also a chance that an uninformed employee

or contractor could expose the company network to danger by giving privileged credentials to an outside threat actor who then uses them to impersonate an insider. The average global cost of insider threats rose to 11.45 US million dollars in the last two years, according to the 2020 Cost of Insider Threats Global Report, and the number of occurrences rose by 47 percent during that time [14]. Therefore, the economic impact of these attacks is severe and countermeasures should be seriously considered. Insider threat has been an issue for national security and global business also. As, we know that technology advancement has boosted the E-Payment globally, it becomes more critical to understand this as the software system advancements brings cyber trouble also. For Example: In February 2016, Bank of Bangladesh, hackers tried to rob 1 billion dollars and they almost succeeded in doing this. They almost attempted to do the biggest Cyber-attack of the history [15].

#### **RQ 2: The common techniques used to carry out insider threats and override controls that are set to detect insider threats in the first place.**

Despite all the work and money put into developing cybersecurity threat detection systems, detecting a malicious activity can take weeks or even more than that. Like, in Bangladesh robbery case, the hackers are still unidentified [16], [17]. However, taking a deep analysis of how an attack is done can help in detecting a cyber-attack. The reason why it's hard to detect a cyber attack is, because most of these are caused by trusted user or ex- employee, who has access to data and resources. According to a data survey from a website, the cost to handle an insider threat is around 8 million dollars on an average [18]. There are numerous ways to carry out insider threats. But the main three of them are:

- i. Data Theft
- ii. Privilege Exploitation
- iii. Sabotage

**I. Data Theft:** it mainly the most popular insider threat widely. There can be numerous reasons for this attack. Ex-employee trying to defame company, Anti company trying to push your company down. The following indicators can be used to detect these types of attacks at first place:

- i. Accessing data when employee is not working.
- ii. Using company's interface on odd device or your personal device.
- iii. Downloading data into your own device.

**II. Privilege Exploitation:** When a employee has access to sensitive information about an organization or company. They can use that information to bring it done or leak it outside. However, it's hard to detect these but there are following ways with which it can be done:

- i. Altering organizations privileges
- ii. Adding new users
- iii. Changing security authentications without any permission.

**III. Sabotage:** This can be defined as a revenge from an employee for being treated unfair or blackmailing the company. This can be detected by following ways:



- i. Constantly keeping an eye on Managers and colleagues' behavior towards another employee.
- ii. Recent argument between employee and company executives
- iii. Requesting access for the privileges that user doesn't need.

### **RQ 3: What methods and techniques are available to overcome and insider threats in the world of cyber security?**

Although, it is hard to eradicate the insider threats issues, but we can use number of ways to minimize it. The fact that we are frequently betrayed by the people we most trust. But still company has to keep faith in their people to run their business smoothly. However, they can use these methods to minimize these and keep track of the attacks.

- i. Company should follow a strict security policy rule, and should form a department that keeps the track of the malicious activities inside and outside the system.
- ii. Infrastructure should be locked with proper security and employee should be given secured lockers to lock their physical and sensitive information and documents.
- iii. The main cause of these activities are mostly the new hires, company should spend money and screening new hires and they shouldn't be given the full authority in the beginning of their job.
- iv. We shouldn't blame humans always for these attacks, our computer system should be secured with auto shutdown system when there is malicious activity or data breach.
- v. Direct employee monitoring is a further helpful tool. You can never be too safe when it comes to your company's confidential information. This can be done using security cameras or implementing keystroke logging.

We can increase the security of the confidential data at our company by putting these insider threat detection techniques into practice. If company is not putting these techniques into action, they may suffer loss of thousands of dollars due to these continuous cyber-attacks. Specially, those in which the insiders are involved and data leak is from inside rather than outside activity.

### **V. FUTURE RESEARCH DIRECTIONS OF INSIDER THREATS**

Based on our research, we presented the following research directions for Insider threats in cyber security.

**i. Threat Type in Cyber Security:** As type of threat, we are dealing with plays a key role in cyber security [19]. If the threat we are dealing is caused by the insider then it is hard to detect and caused high damage to organization also. It is clear that almost every article describes the threat type, but not all of them were able to explain the detection method. As it can be observed that if type of threat is insider, then the loss to company is also high. For example: in case of bank of Bangladesh.

**ii. Behavior Model in Cyber Security:** Modeling the behavior of the user and employee is the another key factor that can help to minimize threats in future. This includes keeping

track of user email activity, log books and their behavior in the organization.

**iii. Threat Detection:** Threat detection helps a company to get a brief info about past attacks and vulnerabilities in the system. We have discussed many techniques used to detect these attacks. Threat detection refers to an IT organization's ability to quickly and accurately detect threats to a network, its applications, or other assets. Understanding the threats that exist in the cyber environment is the first step in developing efficient threat detection and response processes. Organization should have a committee which deals with these attacks and who are ready to take action. So that in future these attacks can be minimized.

**iv. Threat Mitigation:** Threat detection are of no use if organizations are not taking measures to eradicate it. As, discussed in RQ3, company should screen new hires, keep log books of employee data, should follow multi factor authentication. These potential steps can easily help to decrease future cyber attacks on company

### **VI. CONCLUSION AND FUTURE WORK**

This research main focus was on insider threats and its detection. Although, we covered a brief part about cyber security also. The paper highlights the main types and the methods that we can use to minimized those attacks. This research mentions the new discovered methods that has never been used by companies for attack mitigation. Early detection of threats has always been helpful for companies, but most the companies neglect it and loose data and money. Although, it is impossible to completely make a company or system attack-free. Many developments have been made in this field already and more is under progress. The research highlights the potential for future work and the main three agenda are discussed below:

**Potential Research Agenda 1:** Researchers has offers numerous ways of dealing with these insider attacks. However, Use of behavior model techniques to keep an eye on users can be the one of the most efficient techniques for threat detection. Although, researchers still lack in this area as not enough data is available regarding this. Future work could include more deep assessment of human behavior patterns and attacks strategy they use.

**Potential Research Agenda 2:** Several of the study highlighted that insiders' attacks are mainly by the ex- employee or an unhappy user. Future work could include a review of how and why these insiders are influenced to do such things.

**Potential Research Agenda 3:** With the rising of internet and digital world, data transfer is also doubling every year. Out of which, more than half is vulnerable to loss or attacks. Hence, a potential research agenda could be protecting the rising perimeter of internet. For example, to be fully prepared for the worst, organization should invest in comprehensive risk management and compliance solutions. Companies can stay one step ahead of attackers and avoid the worst from ever happening.

## VII. DECLARATIONS OF INTEREST

None.

## VIII. ACKNOWLEDGEMENT

I would also like to extend my deepest gratitude to Professor Ali Dehghantanha for their assistance in completing the project.

## REFERENCES

- [1] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, G. Srivastava, and H. Karimipour, "Secure intelligent fuzzy blockchain framework: Effective threat detection in iot networks," *Computers in Industry*, vol. 144, p. 103801, 2023.
- [2] I. A. Gheyas and A. E. Abdallah, "Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis," *Big data analytics*, vol. 1, no. 1, pp. 1–29, 2016.
- [3] J. Hunker and C. W. Probst, "Insiders and insider threats-an overview of definitions and mitigation techniques," *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, vol. 2, no. 1, pp. 4–27, 2011.
- [4] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, M. Hammoudeh, H. Karimipour, and G. Srivastava, "Block hunter: Federated learning for cyber threat hunting in blockchain-based iiot networks," *IEEE Transactions on Industrial Informatics*, 2022.
- [5] W. Ashford, "Barclays bank leaks thousands of customer records," *Posted Febryary*, vol. 10, 2014.
- [6] A. Yazdinejad, B. Zolfaghari, A. Dehghantanha, H. Karimipour, G. Srivastava, and R. M. Parizi, "Accurate threat hunting in industrial internet of things edge devices," *Digital Communications and Networks*, 2022.
- [7] A. Yazdinejad, M. Kazemi, R. M. Parizi, A. Dehghantanha, and H. Karimipour, "An ensemble deep learning model for cyber threat hunting in industrial internet of things," *Digital Communications and Networks*, 2022.
- [8] M. N. Al-Mhiqani, R. Ahmad, Z. Z. Abidin, W. M. Yassin, A. Hassan, A. N. Mohammad, and N. L. Clarke, "A new taxonomy of insider threats: an initial step in understanding authorised attack," *International Journal of Information Systems and Management*, vol. 1, no. 4, pp. 343–359, 2018.
- [9] S. Walker-Roberts, M. Hammoudeh, and A. Dehghantanha, "A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure," *IEEE Access*, vol. 6, pp. 25167–25177, 2018.
- [10] F. Ullah, M. Edwards, R. Ramdhany, R. Chitchyan, M. Ali Babar, and A. Rashid, "Data exfiltration: A review of external attack vectors and countermeasures," *Journal of Network and Computer Applications*, vol. 101, 11 2017.
- [11] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K. R. Choo, "An energy-efficient sdn controller architecture for iot networks with blockchain-based security," *IEEE Transactions on Services Computing*, vol. 13, no. 4, pp. 625–638, 2020.
- [12] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, and M. Aledhari, "Enabling drones in the internet of things with decentralized blockchain-based security," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6406–6415, 2020.
- [13] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo, "Blockchain-enabled authentication handover with efficient privacy protection in sdn-based 5g networks," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1120–1132, 2019.
- [14] <https://www.tessian.com/blog/insider-threat-statistics/>.
- [15] [https://en.wikipedia.org/wiki/Bangladesh\\_Bank\\_robbery/](https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery/).
- [16] Y. Hailemariam, A. Yazdinejad, R. M. Parizi, G. Srivastava, and A. Dehghantanha, "An empirical evaluation of ai deep explainable tools," in *2020 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–6, IEEE, 2020.
- [17] A. Yazdinejad, B. Zolfaghari, A. Azmoodeh, A. Dehghantanha, H. Karimipour, E. Fraser, A. G. Green, C. Russell, and E. Duncan, "A review on security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures," *Applied Sciences*, vol. 11, no. 16, p. 7518, 2021.
- [18] [www.securityintelligence.com/news/the-average-cost-of-an-/insider-threat-hits-8-7-million/](http://www.securityintelligence.com/news/the-average-cost-of-an-/insider-threat-hits-8-7-million/).
- [19] S. Nakhodchi, B. Zolfaghari, A. Yazdinejad, and A. Dehghantanha, "Steeleye: An application-layer attack detection and attribution model in industrial control systems using semi-deep learning," in *2021 18th International Conference on Privacy, Security and Trust (PST)*, pp. 1–8, IEEE, 2021.

## PRIMARY STUDIES

- [1] Homoliak, I.; Toffalini, F.; Guarnizo, J.; Elovici, Y.; Ochoa, M. Insight into Insiders: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures.
- [2] Kim, J.; Park, M.; Kim, H.; Cho, S.; Kang, P. Insider threat detection based on user behavior modeling and anomaly detection algorithms.
- [3] Ko, L.L.; Divakaran, D.M.; Liao, Y.S.; Thing, V.L.L. Insider threat detection and its future directions. *Int. J. Secur. Netw.*
- [4] Walker-Roberts, S.; Hammoudeh, M.; Dehghantanha, A. A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure.
- [5] Ullah, F.; Edwards, M.; Ramdhany, R.; Chitchyan, R.; Babar, M.A.; Rashid, A. Data exfiltration: A review of external attack vectors and countermeasures
- [6] Liu, L.; De Vel, O.; Han, Q.-L.; Zhang, J.; Xiang, Y. Detecting and Preventing Cyber Insider Threats: A Survey. *IEEE Commun. Surv. Tutor*
- [7] Nazir, S.; Patel, S.; Patel, D. Assessing and augmenting SCADA cyber security: A survey of techniques. *Comput. Secur*
- [8] Farahmand, F.; Spafford, E.H. Understanding insiders: An analysis of risk-taking behavior. *Inf. Syst. Front.*
- [9] Trustworthiness Attribution: Inquiry Into Insider Threat Detection. *J. Assoc. Inf. Sci. Technol*
- [10] Alneyadi, S.; Sithirasanen, E.; Muthukkumarasamy, V. A survey on data leakage prevention systems. *J. Netw. Comput.*
- [11] Crossler, R.E.; Johnston, A.C.; Lowry, P.B.; Hu, Q.; Warkentin, M.; Baskerville, R. Future directions for behavioral information security research. *Comput. Secur*
- [12] Magklaras, G.B.; Furnell, S.M. Insider Threat Prediction Tool: Evaluating the probability of IT misuse. *Comput. Secur*
- [13] Gunasekhar, T.; Rao, K.T.; Basu, M.T. Understanding insider attack problem and scope in cloud. In *Proceedings of the Power and Computing Technologies (ICCPCT)*, Nagercoil, India
- [14] Xiaojun, C.; Zicheng, W.; Yiguo, P.; Jinqiao, S. A Continuous Re-Authentication Approach Using Ensemble Learning. *Procedia Comput. Sci.*
- [15] Leu, F.Y.; Tsai, K.L.; Hsiao, Y.T.; Yang, C.T. An internal intrusion detection and protection system by using data mining and forensic techniques. *IEEE Syst. J.*
- [16] Maestre Vidal, J.; Lucila Sandoval Orozco, A.; Javier García Villalba, L. Online masquerade detection resistant to mimicry. *Expert Syst.*
- [17] Parveen, P.; McDaniel, N.; Weger, Z.; Evans, J.; Thuraishingham, B.; Hamlen, K.; Khan, L. Evolving insider threat detection stream mining perspective.
- [18] Nasr, P.M.; Yazdian-Varjani, A. Toward Operator Access Management in SCADA System: Deontological Threats Mitigation. *IEEE Trans. Ind. Inform*
- [19] Clark, J.; Leblanc, S.; Knight, S. Compromise through USB-based Hardware Trojan Horse device. *Futur. Gener. Comput. Syst*
- [20] Punithavathani, D.S.; Sujatha, K.; Jain, J.M. Surveillance of anomaly and misuse in critical networks to counter insider threats using computational intelligence. *Cluster Comput.*
- [21] Rajamanickam, S.; Vollala, S.; Amin, R.; Ramasubramanian, N. Insider Attack Protection: Lightweight Password-Based Authentication Techniques Using ECC. *IEEE Syst. J*
- [22] Li, W.; Meng, W.; Kwok, L.F.; IP, H.H.S. Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model. *J.*
- [23] Bostani, H.; Sheikhan, M. Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach.
- [24] Shu, T.; Krunz, M. Privacy-preserving and truthful detection of packet dropping attacks in wireless ad hoc networks. *IEEE Trans. Mob. Comput.*
- [25] Yan, Z.; Ding, W.; Niemi, V.; Vasilakos, A.V. Two Schemes of Privacy-Preserving Trust Evaluation. *Futur. Gener. Comput. Syst*



- [26] Rrushi, J.L. NIC displays to thwart malware attacks mounted from within the OS. *Comput. Secur.*
- [27] Sandhu, R.; Sohal, A.S.; Sood, S.K. Identification of malicious edge devices in fog computing environments. *Inf. Secur. J.*
- [28] Huayu, F.; Jun, H.; Menglin, W. Research on fog computing based active anti-theft technology. *Procedia Comput. Sci.*
- [29] Lopez, J.; Alcaraz, C.; Roman, R. Smart control of operational threats in control substations
- [30] Callegati, F.; Giallorenzo, S.; Melis, A.; Prandini, M. Cloud-of-Things meets Mobility-as-a-Service: An insider threat perspective. *Comput. Secur.*
- [31] Cho, J.H.; Chen, I.R. Performance analysis of hierarchical group key management integrated with adaptive intrusion detection in mobile ad hoc networks
- [32] Kim, J.S. Development of integrated insider attack detection system using intelligent packet filtering. In *Proceedings of the 2011 First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering*
- [33] Rose, I.; Felts, N.; George, A.; Miller, E.; Planck, M. Something Is Better Than Everything: A Distributed Approach to Audit Log Anomaly Detection. In *Proceedings of the 2017 IEEE Cybersecurity Development (SecDev)*
- [34] Meryem, A.; Samira, D.; Bouabid, E.O.; Mouad, L. A novel approach in detecting intrusions using NSLKDD database and MapReduce programming
- [35] Böse, B.; Avasarala, B.; Tirthapura, S.; Chung, Y.Y.; Steiner, D. Detecting Insider Threats Using RADISH: A System for Real-Time Anomaly Detection in Heterogeneous Data Streams. *IEEE Syst. J.*
- [36] Lo, O.; Buchanan, W.J.; Griffiths, P.; Macfarlane, R. Distance Measurement Methods for Improved Insider Threat Detection. *Secur. Commun. Netw.*
- [37] Chen, Y.; Nyemba, S.; Malin, B. Detecting Anomalous Insiders in Collaborative Information Systems. *IEEE Trans. Dependable Secur. Comput.* 2012
- [38] Mayhew, M.; Atighetchi, M.; Adler, A.; Greenstadt, R. Use of machine learning in big data analytics for insider threat detection. In *Proceedings of the MILCOM 2015–2015 IEEE Military Communications Conference*, IEEE, Tampa, FL, USA, 26–28 October 2015
- [39] Shemla, A.; Bineesh, V. An EvABCD approach for masquerade detection. In *Proceedings of the Second International Conference on Current Trends In Engineering and Technology-ICCTET 2014*, IEEE, Coimbatore, India, 8 July 2014;
- [40] Mohan, R.; Vaidehi, V.; A, A.K.; Mahalakshmi, M.; Chakkaravarthy, S.S. Complex Event Processing based Hybrid Intrusion Detection System. In *Proceedings of the 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN)*, Chennai, India, 26–28 March 2015
- [41] Mtibaa, A.; Harras, K.; Alnuweiri, H. Friend or Foe? Detecting and Isolating Malicious Nodes in Mobile Edge Computing Platforms. In *Proceedings of the 2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom)*, Vancouver, BC, Canada, 30 November–3 December 2015
- [42] Lopez, J.; Alcaraz, C.; Roman, R. Smart control of operational threats in control substations. *Comput. Secur.* 2013
- [43] Meng, W.; Luo, X.; Li, W.; Li, Y. Design and Evaluation of Advanced Collusion Attacks on Collaborative Intrusion Detection Networks in Practice. In *Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA*, Tianjin, China, 23–26 August 2016
- [44] Liu, A.Y.; Lam, D.N. Using Consensus Clustering for Multi-view Anomaly Detection. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy Workshops*, San Francisco, CA, USA, 24–25 May 2012
- [45] Gupta, S.; Hanson, C.; Gunter, C.A.; Frank, M.; Liebovitz, D.; Malin, B. Modeling and detecting anomalous topic access. In *Proceedings of the 2013 IEEE International Conference on Intelligence and Security Informatics*, Seattle, WA, USA, 4–7 June 2013;
- [46] Brdiczka, O.; Liu, J.; Price, B.; Shen, J.; Patil, A.; Chow, R.; Bart, E.; Ducheneaut, N. Proactive insider threat detection through graph learning and psychological context. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy Workshops*, IEEE, San Francisco, CA, USA, 24–25 May 2012
- [47] Kandias, M.; Gritzalis, D.; Stavrou, V.; Nikoloulis, K. Stress level detection via OSN usage pattern and chronicity analysis: An OSINT threat intelligence module. *Comput. Secur.* 2017,
- [48] Agrafiotis, I.; Erola, A.; Happa, J.; Goldsmith, M.; Creese, S. Validating an Insider Threat Detection System: A Real Scenario Perspective. In *Proceedings of the 2016 IEEE Security and Privacy Workshops (SPW)*, IEEE, Boston, MA, USA, 22–26 May 2016
- [49] Berk, V.H.; Cybenko, G.; Gregorio-De Souza, I.; Murphy, J.P. Managing malicious insider risk through BANDIT. In *Proceedings of the 2012 45th Hawaii International Conference on System Sciences*, IEEE, Maui, HI, USA, 4–7 January 2012;
- [50] El Anbal, M.; Abou El Kalam, A.; Benhadou, S.; Moutaouakkil, F.; Medromi, H. Securing SCADA Critical Network Against Internal. In *Proceedings of the International Conference on Critical Information Infrastructures Security*; Springer: New York, NY, USA, 2017