Insider threats and Insider Intrusion Detection

Lekshmipriya S B, G Geetha

Abstract: ***this survey paper narrates insider threats and their detection types and methods. Insider threats are emerging nowadays, it is important to identify these threats as they are generating critical problems to the system. This paper pays particular attention to the categories of threats and different types of detection methods. Based on different strategies, statistical and machine learning methods for detecting these threats, are identified and summarized here.***

***Index Terms*: *Security, Insider threats, IDS*.**

I. INTRODUCTION

This paper presents the literature survey of insider threats, their intrusion detection methods and risk analysis. Statistical and machine learning methods for detection of insider threats are described. Different types of strategies for classification and algorithms for detection are also discussed.

Cyber security is one of the most popular terms in this communication world. It encompasses a set of methods, technologies to protect systems, networks, and data from unauthorized access, modification, or destruction. Intrusions are mainly two types, internal intrusion and external intrusion. Internal threats are more threatening than external threats. There is no clear evidence for internal threats. They are more damaging than the external threats [1]. It is difficult to identify these insider threats, but when it come into being the result or the damage is monumental [2].A survey conducted by US State of Cybercrime survey and CERT in 2016 states that around 27% of the threats are insider threats. But those threats are not under estimable, its damage is tremendous. As the insiders know the credential of the system it is easy to exploit the system without breaking the system [3].There is mainly two type's insider threats, intended malicious activities and careless user errors [1].The Insider Threat Blog by CERT in 2019 explained that about 78% of the threats are intentional and 22% of the remaining threats are careless errors within the specified organizations [4].

Insiders are employees or persons who is having the credentials with the right to access the assets of an organization. [5].A detailed classification of insider threats are human threat, environmental threat and technological threat. Human threat is again classified into malicious and non-malicious threats. The malicious threats are again classified into accidental and intentional. Environmental threats and technological threats are non-malicious, they are also unintentional [6].Insider threat classification can be concluded into three most common types of insiders namely traitor, masquerader and unintentional perpetrator.

The insiders, who are traitors, having the characteristic of making their attacks by using their passwords (as they are legitimate users) and act as adversarial to the system that hits the CIA properties of the system. It will cause harm to the system. Masqueraders are the insiders, who attacks the system by stealing the credentials from authorized/legitimate users and pretense as another user and launches the attacks. Unintentional penetrators are careless user who lacks the security awareness

The common attacks occurred by insiders are unauthorized access, data replication or data exfiltration, unauthorized modification, deletion of documents, downloading data from unauthorized sources, sharing of unauthorized data, data, IP spoofing, masquerading , misuse of resources and malicious software installation [7].

Security system is mainly classified into host and network security systems. Each of these security system needs at a minimum, a firewall, antivirus software, and an intrusion detection system. IDSs helps to understand, determine, and identify unauthorized use, duplication, modification, and destruction of information systems [8].

There are three main types of cyber analytics in support of IDSs: misuse-based, anomaly-based, and hybrid. In misuse based techniques, the known attacks are detected by using the signatures of those attacks which is already stored in the database, with less false alarms. It can be acquire if frequent updates of database is available. It is used for known attacks and zero-day vulnerabilities cannot be detected by this techniques. Anomaly-based techniques identifies anomalies from network and system behaviors. They are captivating because of their ability to detect zero-day vulnerabilities. Main disadvantages of this system is high false alarm rates as it is considering new system or network behaviors also as anomalies. Hybrid techniques combine misuse and anomaly detection. They are exerted to raise detection rates of known intrusions and decrease the false positive rate for unknown/new attacks.

The data sources are mainly classified into host based, network based and contextual based. [9]. Typical host-based data sources include system calls (homogenous or heterogeneous), keyboard and mouse strokes, unix shell commands and host logs. Network traffic and logs,IP address,TCP flows are the most common example for network-based data source, from which information can be extracted to modelling the networking behaviors of any users [10].Contextual data source provide contextual information such as the human resources (HR) and psychological data of a human

Revised Manuscript Received on July 22, 2019.

Lekshmipriya S B, Research scholar, Computer Science and Engineering, Jerusalem College of Engineering, Anna University, Chennai, India.

Dr.G Geetha, Professor, Computer Science and Engineering, Jerusalem College of Engineering, Anna University, Chennai, India.

user. Contextual data sources have shown great potential in conducting intent analysis and validating the suspicious behaviors reported by a conventional analytics [11]

II. CLASSIFICATION OF INSIDER THREATS

Insider threats are classified based on several criteria. Malicious and non-malicious insider threats are seen as the common insider threat

A. Multi-dimensional Classification

Multi-dimensional model is a combined model based on attack techniques and threat impacts [6].Three dimensional or orthogonal model (This model classifies threats by using the labels, agent (human or technological), motivation (intentional or unintentional) and localization (represents the origin whether insider the perimeter or not)[7],Pyramid model(It classifies the intentional threats (human threats) based on attacker's prior knowledge about the system, criticality of the area and loss, Information system security threat cube classification model(Based on the features like security threat frequency, area of security threat activity, security threat source, the model is classified) are some models which is classified based on attack techniques. Classification based on threat impacts includes the models like STRIDE model (This model can be used for network, host and its application. It characterizes attack based on the motivation of attacks (STRIDE is spoofing, Tampering data, Repudiation, DOS, and Elevation of privilege))[8]and ISO model (The five threat impacts are Destruction of information, corruption of information, theft, removal of information, disclosure of information).Multi-dimensional model classifies both internal and external threats. The source is considered as within the organization and outside the organization.

1) Based on Security threat source

Insider threats occurs when someone has achieved the credentials, due to flaws like employee action or failure of organization process.it can be classified based on the source, whether it is internal or external

2) Based on Security threat agent

Based on security threat agent behavior threats can be classified into human threats, technological threats and environmental threats. Agent is an actor which impose threat to the system [6]

a) Human threats.

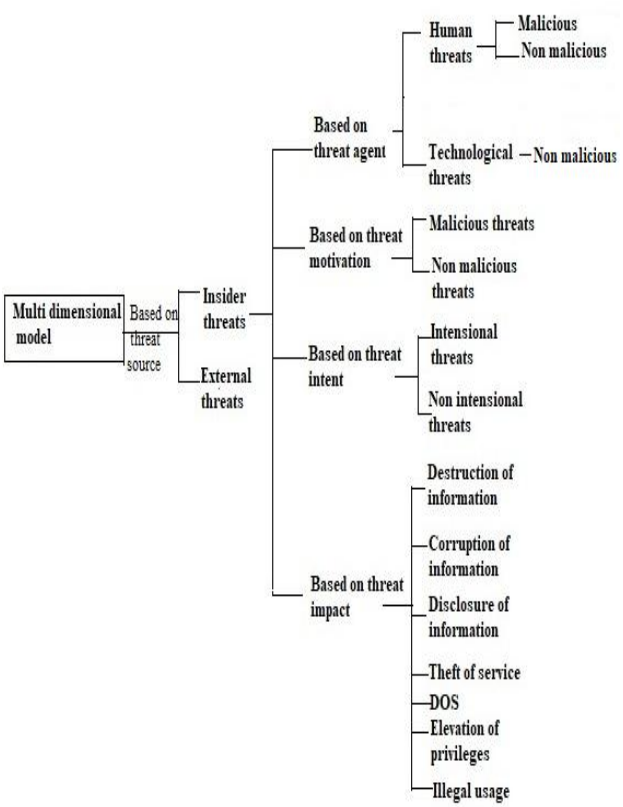
It is done by insider or hackers which harm the system. Human threats are most harmful to the system. Different types of human threats are intentional and unintentional.

b) Technological threats

It is caused by physical and chemical processes on the materials. Another threats are like getting entry to the restricted areas and causing theft or damage to the software or hardware

3) Threat motivation

Attackers should have a motive for attacking the system. This may result in a binary classification of the threats. This motive may results in malicious (inserting virus and Trojan horse) and non-malicious (vulnerabilities due to poor security policies)



4) Threat intent

This binary classification of threats shows whether it is intentional or unintentional.

Intentional threats: It happens when someone purposefully damages the information like IP theft, credit card crime

Unintentional threats: it happens without awareness like accidental modification of software, corruption of data

5) Threat impact

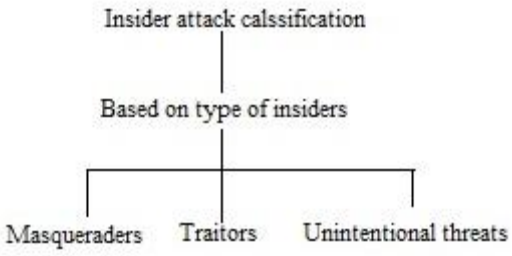
Threat impact is mainly seven types whether it is intentional or unintentional. They are destruction of information, corruption of information, Disclosure of information, Theft of service, DOS, Elevation of privileges and illegal usage

B. Based on Type of Insider

1) Masquerader

Advanced persistent threat (APT) intrusion kill chain [12] represents a latest intrusion campaign paradigm, it is used in this survey to explain the early-stage threats posed during the brooding period of a masquerader. Reconnaissance includes the following threats, network vulnerability scan, web application vulnerability scan, port scan, database vulnerability scan, Social engineering threats includes in

weaponization. In delivery, threats like Email spam (URL or attachments) malicious or phishing websites, removable media exploit, privilege escalation are follows. RAT or backdoor are the threats occurs in the install stage.C2 stage includes DDoS, Email spam, Click fraud and bit coin mining [9]



2) Traitors and Unintentional penetrators

Traitors and unintentional threats will be activated only at the last stage i.e. the action on objectives. These threats includes data exfiltration, violation against data integrity or data availability, sabotage

C. Based on Behavioral Class

This insider threats are classified into masquerading, information theft, collusion and sabotage respectively to the following behaviors. The behavior classes [13] corresponding to the threats are

1) Biometric behavior

Biometric behaviors can be used to differentiate between individuals. By monitoring and recording and testing each employee's behavior for inconsistencies across time, it can be useful for detecting masqueraders, who are employees masquerading (uses another coworker's identify) as another user to carry out malicious. Biometric behavior includes the cyber and physical behaviors. Both of them can cause masquerading [14].

a) Cyber behavior

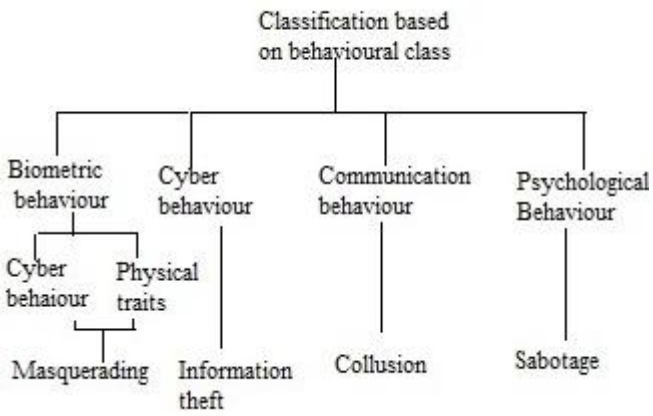
Keyboard and mouse strokes, file search are few cyber behaviors, variation of these features provides the information of threats.

b) Physical traits

Eye color, face recognition, thump print are some physical features, which are normally shows variations and provides the information.

2) Cyber behavior

Printing, web browsing, login behavior, file access are common cyber behaviors. There is no clear distinction between biometric behaviors and cyber behaviors; each individual can be identified by biometric behavior, while cyber behaviors often cannot.



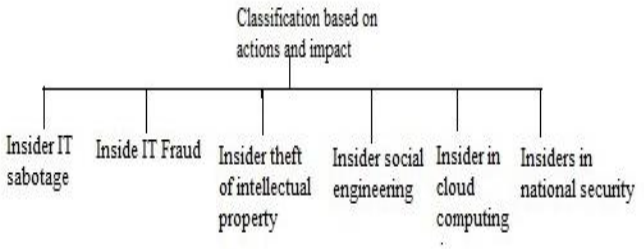
3) Communication behavior

Communication behaviors are behaviors that describe communication between employees. These behaviors can be extracted from the email, instant message, telephone, and file-sharing transfer between individuals

4) Psychosocial behavior

Psychosocial behaviors are behaviors which can be used to detect saboteurs, who are disgruntled employees who sabotage the integrity of their organization, such as planting scripts, spoofing, compromising computer accounts and creating backdoor accounts. Saboteurs Friendliness, attitude against authority, social media behavior are few psychological behaviors [15].

D. Based on Actions and Impact



1) Insider information technology Sabotage

In these attacks insiders uses their experience and knowledge to exploit the system and launch an attack on an individual or an organizations. Attackers mainly targets systems, and employees while they are under stress, or pressure from their boss or organization. Most probably the saboteurs are former or disgruntled employees who is not having the credentials and they are working remotely, than the normal hours, and making their own plans to exploit the system mainly databases, and network devices [15].

2) Insider IT fraud

Insider IT fraud are the insiders who is having the credentials for authorized access. They used their power

for their personal gain by creating deleting, modifying and even selling the confidential information. These insiders are generally current employees, working in normal hours. Their main target is information asset, and they affect the integrity and confidentiality of data also.

3) Insider Theft of Intellectual Property

Insider theft of intellectual property are insiders who steal information which is created by the organization who employs him. They are generally current employees or the employees in their resignation notice period and still having the authorized access. They do not need tools to launch attack. They normally steal information about the source codes, business plans and customer information [15].

4) Insider Social Engineering

In Insider social engineering (SE) the attackers psychologically influence another innocent employees without their knowledge and grabbing the confidential information regarding the organization or make them to harm the organization. These threats occur when these attackers do not having the authorization to access the assets. It may be multiple stage attack, if they are not having the credentials they may use phishing tools to launch the attacks i.e. finding out the usernames and passwords for the data bases ,services and devices the part of individual who do not have authorization access to target systems, and uses phishing tools to launch the attacks. The main targets are access usernames and passwords, systems, services, and network devices. [16]

5) Insider in Cloud Computing

Insider in cloud computing are attackers those working inside service provider company environments, and they attacks the data assets confidentiality without the knowledge of client. There are no effective methods or tools to prevent these types of attacks. They are generally the current employee's works in technical positions and a clear knowledge and a motive and they are legitimate users also. The main insider targets are data assets such as databases, source codes, business and strategic plans [17].

6) Insiders in National Security

These threats involve an insider, who is having the authorized access, do harm to a country's national security. This threat can cause damages through espionage, sabotage, disclosure of national security information, or through the loss or degradation of departmental resources or capabilities. Their main targets are the national security secret information.

III. INSIDER THREAT DETECTION SYSTEMS

A. Classification Based on Architecture

The architecture of an IDS can affect its overall performance, thus is an important decision during the system's design [18]. This is essential for most organizations (companies, universities) due to the high speed network.

1) Centralized

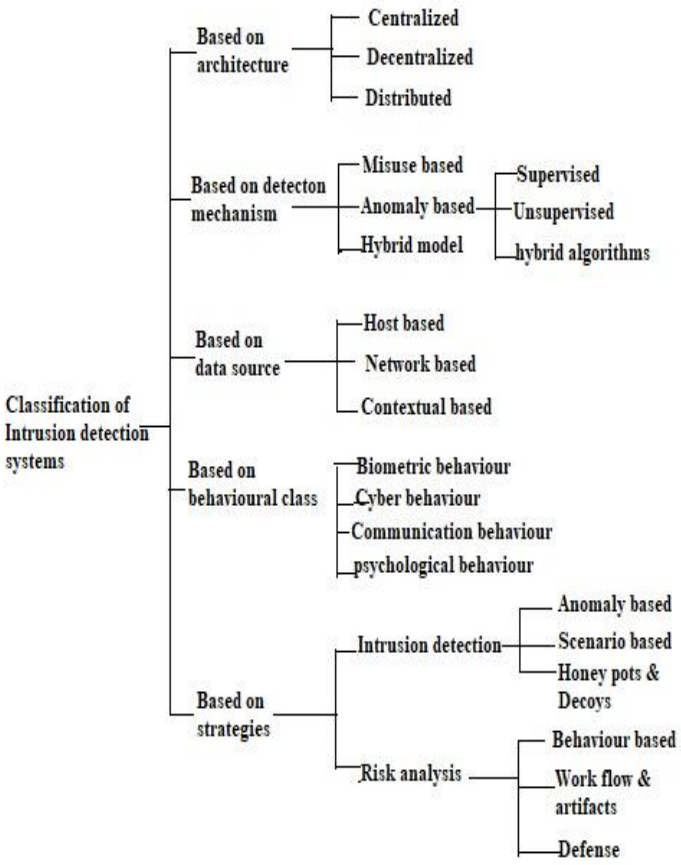
Centralized IDS having multiple sensors across the network and they sends the data directly to CPU. The collected data is analyzed and detected by the CPU. But it does not provide the scalability

2) Decentralized

It is a hierarchical structure of multi sensors and multi-processing units. Collected data is transferred to the nearest processing unit and got processed before reaching the main CPU. It is Scalable.

3) Distributed

In this multiple autonomous agents act as sensors and processing units at the same time. Data collected and processes by those agents than CPU and communicate through P2P architecture. Loss of communication between the agents may lead to inability of finding distributed attacks



B. Based on Detection Mechanism

1) Misuse based

In misuse based detection mechanism systems maintain a database of predefined signatures that correspond to known attacks and perform the detection by comparing these to the data stream [9].SNORT and BRO are two of signature based open source IDS commonly used in enterprise levels, but they are consuming large amount of resources like CPU and memory. The performance of a misuse intrusion detection system is linked with the quality of its database [19]. Low false positive rate is the main advantage of these systems. Nowadays there are

more attacks and variations, maintaining a perfect updated set of rules are not feasible. If so, there is also time wastage and insufficiency will occur.

2) Anomaly based

Anomaly-based IDSs do not depend on previously defined patterns, but they models the normal behavior in order to find out the abnormal behavior, so they are can give a better detection of both known and unknown attacks.

Anomaly-based IDS can be divided into the following categories according to the method they use: supervised (classification), unsupervised (clustering and outlier detection), and hybrid model [18].

a) Supervised IDS

In supervised IDS, a model is trained using the data (labelled).When the new instances are introduced to the model, the classifier will categorizes it into one of the pre-defined classes. By using C$4.5 algorithm (Decision tree algorithm is based on the concept of information entropy for creating an if-then rule at each tree node in order to build the tree. This algorithm require labelled training data for at least two classes), supervised algorithms can produce better results in false positive i.e. Low false positives while considering the unknown attacks SVM [20] produced better results.

b) Unsupervised IDS

Unsupervised algorithms uses the clustering techniques. They are able to identify possible threats, without having any prior knowledge. Clustering separates finite unlabeled data into in finite natural hidden data structures. A score is assigned for each clusters, if the score of the clusters are more than the predefined threshold it is considered as anomalous. Another important part of the unsupervised anomaly detection is feature selection. Feature selection is the process of selecting a subset of the available features that are the most significant and less redundant.ie, the feature extraction aims to create new features of higher quality. Both processes can affect not only a system's detection rate.

Graph based data are unsupervised algorithms that can be used to uncover the graph-based anomalies: modifications, insertions and deletions [21]. The concept behind the graph based approach is, anomalous substructure is a part of non-anomalous or normative sub structure. GBAD-MDL (for anomalous graph modification), GBAD-P (for anomalous insertions), and GBAD-MPS (for anomalous graph deletions) are used for detecting anomalies. These algorithms uses SUBDUE to discover the most prevalent substructure, or normative pattern. In MDL it finds out the best sub structure, and finds out all the sub structures which are closest to that sub structure. The sub structures which are closest to it is non anomalous or normative. The lower the value of multiple of cost of transformation and frequency, the more anomalous the structure. GBAD-P is the probability algorithm which also used MDL, examines all extensions to the normal patterns and need to find the extension with lowest probability. GBAD-maximum partial sub structure also uses MDL, it examines the extensions of all parent structures that are missing edges ad vertices. The instance with lowest cost of information and lowest frequency is considered as anomaly. It is done with only normative pattern. Normative pattern of different persons are different. For example normative pattern of one customer is not same as another customer's pattern in a graph of telephone calls.

c) Hybrid

This is a combination of supervised and unsupervised algorithms. Multi-step outlier detection include a mutual information and generalized entropy feature selection, a tree based subspace clustering technique called Tree CLUS (TCLUS) and an anomaly detection, based on the ROS' score[22].This methodology outperformed high detection rate in Normal and U2R classes. An intrusion detection system that uses K-means, SVM and fuzzy neural networks consists of four stages. K-means is used to generate training clusters from the initial dataset. Neuro-fuzzy model is trained for each training set and subsequently a vector for SVM classification is generated and SVM classifier is used to detect the attacks. This method has high rates in the two low-frequency attack classes, U2R and R2L.

3) Hybrid model

Combination of multiplied techniques is helping to inherit the advantages of those algorithms together; therefore they are able to improve the detection rate and minimizing the false positives. The combination of the C4.5 decision tree and multiple one-class Support Vector Machines (SVMs) to model normal behaviors [23].Random forest methods are used hybrid intrusion detection systems [24].

C. Based on Data Source

There is mainly three types of data sources in Intrusion detection system [9] .They are a) host based intrusion detection system, network based intrusion detection system, and Contextual based Intrusion detection System

1) Host based Analytics

In host-based analytics, the data source is mainly the host and the data ranges from operating system low-level data such as system calls to application-level data such as keystroke or mouse dynamics. When the data source is system call sequence, intrusions and malwares are the commonly occurring threats. The algorithms generally used are statistical(n gram model and sequence match algorithms),machine learning(n gram model and feed forward neural networks)and deep learning(n gram model and recurrent neural network ,statistical(frequency model ,LR) and machine learning algorithms(KNN,SVM) are used. While considering the system call parameter, the threat type is specifically insider intrusion. The algorithms used are, signature based algorithm [25] and minimum description length algorithm. The n-gram based techniques fully utilized the temporal correlation come across in system call sequence and the non-linearity property of ANN. But it will consistently increasing computational complexity. A mix of the two models may achieve a better balance between scalability and effectiveness.

a) Command sequence, key board and mouse stroke

Sequence and frequency models are used here. Statistical (Sequence match, Bayes factor test), machine learning (Naïve Bayes, SVM, ANN) and fuzzy systems (fuzzy user profile) are served. Keyboard and mouse dynamics is also a valid data source for conducting analysis behavioral biometrics [26] creates a user profile with features extracted from the dynamic behavior. The features like flight time, which are unique for each individual are key features for characterizing keystroke dynamics, which are known to be very unique for every individual. In regard of mouse dynamics, the average speed against travel distance and movement direction are worked out as the features. An ANN is trained with these features, according to which any inconsistent dynamics will indicate the existence of a masquerader.

b) Host logs.

Operating system's logging capability allows to record any events either occurs in an operating system or other software/programs run, or messages communicated between different users. They have provided many data sources for auditing and tracing a host's behavior and, therefore, are quite suitable for detecting intrusions, malware and malicious insiders. Insider threats are generally occurs from the win system log data sources. Statistical (GMM, KDE) and machine learning algorithms (SVM) are surveyed. The Gaussian mixture model (GMM), SVM and kernel density estimation (KDE) are all experimented with a few of the most significant features which, finally, concludes that the GMM outperforms the others [27].

2) Network based Analytics

Routers, switches, load balancers and firewalls have the ability to collect the network traffic passing through which, are considered the major audit data sources for detecting intrusions [28] and the network logs have great potential for addressing insider threats. Several classification algorithms, like Decision tree, Support Vector machine-Nearest Neighbor, Bayes Classifier, Neural Networks, Recurrent neural networks etc., have been used for network based intrusion detection. Traffic based analytics and network logs are used as the data sources [9]

a) Traffic based analytics

These analytics are traditionally developed for intrusion detection .DNS traffic, IRC traffic, HTTP traffic, Netflow are the mainly used data sources here. If two groups of IP address access a same domain name at different times and their similarity is more than a threshold, this domain name is labelled as suspicious. Demolishing a botnet prevents an attacker from further threats, the schemes can only be used as compromised solutions for inscribing insider threats. Due to the complexity of network traffic, machine learning and statistical algorithms are most widely used and they very effective also

b) Network logs

Proxy logs, Email, LDAP logs as used input to Markov model, KDE,GMM statistical methods ,proxy, LDAP, DHCP, VPN logs are given as input to KNN,KMC algorithms and also proxy, Email logs are given as input for the RNN deep learning networks[29]. By looking at the web server logs, log management system along with the detection methods can unauthorized access and automated activities resulting from malicious insiders. A normative pattern (a graph substructure) is learnt from the entire graph that describes an insider's correspondences by using MDL and can find the anomalies. Each rule [30] is meant to express a specific type of unusual insider activity regarding email communications. Beehive is very effective against unusual behaviors caused by adware, malware, policy violations and other suspicious activities (subject to manual investigation). There is also a graph-based system proposed to address insider threats.

3) Contextual based Data analytics

HR data, network data, host data, psychological data are the data sources for contextual data analysis. The algorithms used are rule-based (signature match), Statistical (KDE), graph-based (bipartite graph), conceptual framework (network factor analysis scoring graph-based (SAD) machine learning (Bayesian) [31]

a) HR data

HR data are data that contain employment related information (as name, office location, job description) in an organization, these are critical information for behavioral data analysis. A number of hand coded rules and the KDE based algorithms are employed as sub-detectors. Each user is having a threat score, Bayesian network that aggregates all the alerts threat score is generated for each user s triggered by the sub-detectors .Graph based algorithms are also used to detect insider threats ,in which users normal behavior is plotted as bipartite graph. According to their role. Each workgroup role's normal and expected behaviors. If any user conducts any out-of-scope behaviors in terms of his/her workgroup role, an alert will be triggered.

b) Psychological data

Employee's feelings and attitude about the organization are considered as psychological data and it will tend as insider threats. It will be more effective in hybrid models. If the user's behavior is suspicious in host based analytics, it is good to check the psychological data and detect the find out whether it is malicious. [9]

D. Based on Behavioral Class

1) Biometric behavior

Generally, the approaches used to detect insider threats are analyzing the employee behaviors and identities. Different behaviors are suited for detecting different types of attacks. Biometric behaviors like keyboard and mouse strokes are useful for identifying masquerading, Communication behaviors like email are useful for detecting collusion, while file-access behaviors are useful for detecting information theft and psychological behaviors like social media behaviors are

useful for detecting sabotages [13].

a) File search behavior

The commonly used algorithms for file search behaviors are one class support vector machine, Naive Bayes, support vector machine, KNN, similarity measure. One class support vector machine uses the input features like no of search related requests, file access with each two minute epoch, and it provides 100% TPR at 1.1% FPR.Naive Bayes provides 100% TPR and 1.8% FPR, Support vector machine (No of file access, average time between file access, depth of file search, path distance between accessed files within the file directory) provides 87.9%TPR and 20.1 FPR and KNN [88.7%TPR and17.0 %FPR]

b) System level behavior

GMM used the no of unique process, processes created, processed, destroyed, files touched, and windows focus actions as input results .78 AUC .Another algorithm used is oc-SVM with same input features provides .71 AUC.

c) UNIX command behavior

UNIX commands are mainly classified into two types. Truncated (main commands) and Enriched commands (command arguments and time stamps).Pattern mining, Frequency distribution, Co-occurrence matrix, Sequence matching, Compression, Markov model are used with 1% FPR and at 3% FPR. The result of TPR at 1% are 70%,65%,55%,50%,40%,30% respectively. The results at 3% are 90%, 85%, 80%, 65%, 60%, and 60% respectively.

2) Cyber behavior

Cyber behaviors includes Printing, web browsing, login behavior, file access. The algorithms used are Naive Bayes and Relational pseudo Anomaly detection. Naive Bayes used the input features search, browse, download, print behaviors such as no. of remote print job, no. of queries made during a suspicious time, no of queries that results in high documents retrievals results .92 AUC. Relational pseudo Anomaly detection(input features like email, file ,group, login, printer, URL behaviors such as mail attachments ,no of file to removable device, no of shared printers)provides .98 AUC

3) Communication behavior

Frequency based and scan based approaches which includes Scan statistics, Edge node ratio of vertices in communication graph structure, Anomalous communication graph structure algorithms are used

4) Psychosocial behavior

Random forest algorithm (with data source, guild leaving activities in online game platform and features are friendliness, measured as centrality of the character in social network graph) results 90% TPR. Naive Bayes, SVM, logistic Regression with same data source results 81% F-score. Bayesian network with grading of behavior by human resource personal shows .18 RMSE while the same algorithm with a data source of self-evaluation of likelihood of displaying bad behaviors, with 12 psychological features shows 60% FPR.

E. Based on Strategies

Insider threat research is mainly classified into Intrusion detection, Risk Analysis, Testing and synthetic data Generation, and Process control. Intrusion Detection included the Anomaly based detection, Scenario based intrusion detection, Use of honeypots and decoys, Indicator based intrusion detection. The Risk analysis includes indicator based, Behavioral based, Work flow and artifacts, Defense. Defense is again classified into Network strengthening and Role based access control [32]

1) Anomaly based detection

Basic idea between anomaly detection is comparing the observed data to the data the normal behavior. If any abnormalities it is consider as anomalies. In RPAD, the observed data instances are considered as non-anomalous and constructing equal number of pseudo anomalies from a joint distribution .In RPAD, a classifier distinguish between data observations and pseudo anomalies. RPAD combines the classifiers prediction with pseudo anomaly distribution to determine whether the instance is anomalous. This approach produces a representation of the joint distribution that is sufficient for anomaly detection [33] Relational Density Estimation (RDE) RDE is also uses the joint probability.in this joint probability is assumed to be simple product of marginal distribution. The marginal density is modelled using kernel density estimator. Anomalous points are the points which is having low probability estimates under joint distribution.

2) Scenario based intrusion detection

Proactive Detection of Insider threats with Graph Analysis and Learning, has applied and evaluated multiple Anomaly Detection algorithms. Different aspects of user behavior; like domain knowledge, structural features like graph based features and visual Ad language is also used here. Starting points are indicators, anomalies and scenarios. This framework is a combinations of features, entities, baselines and detection methods for ITs. A visual AD language is created which enables the expression of combinations of methods, data, baselines, and detection extents. The language specifies both the extent of the entities to be detected (e.g., individual users or groups of users) and the temporal extent of potential anomalies

IP Thief Ambitious Leader Scenario detector issued [34], the detector completely ignores 33 user-days which does not fit with its assumptions. File Events indicator method, users who display abnormal behavior with respect to files, focusing on file events related to removable media drives and the number of distinct files that a user accesses. It ignores user-days with no removable drive activity. Relational Pseudo Anomaly Detection Results from RPAD were highly consistent during the period. Feature normalization resulted in very high performance with .97 AUC. Repeated Impossible Discrimination Ensemble RIDE was also consistent at same period. Each user's aggregate is compared to other users aggregate and represented by the degree of statistical anomaly. This provides the best result for AUC while comparing with other AD algorithms.

3) Use of honeypots

Honey-tokens are method which is used to attract malicious insiders, and helps to detect, identify and confirm a malicious insider threat [35].It could be a digital entity and it is a technique that is a part honeypot technology. However, it is different to other types because it could be any interactive digital entity. No one should interact with the honey token and if any interaction with it, it will indicate to the security administrator that there could be the threat

4) Behavior based Intrusion detection

In this detection technique, psychological signals of human are used. Sudden abnormalities of psychological signal while handling sensitive information during working with the system. It results in a detection of malicious activities. Normal behaviors of participants are noted as the baseline. Once it is recorded employees are given systems and recorded the psychological signals like temperature, ECG. Continuous physiological signals monitory system is needed. If the person does not feel fear or stress, this method is out of scope [36]

5) Workflow and Artifacts

Risk analysis using work flow includes abstraction of various communication channels and hence is flexible to develop insider threat detection technology. This is gained by modeling a user's view of the organization and capability detects the insider threats.

6) Defense

Improving defense of the network or the data or by improving it by access control etc. are comes under defense. It includes some prevention methods like "requires/provides" model based on attack trees which can be used to defend against insider attacks, though such methods rely heavily on the defenders' capabilities and knowledge of the environment.

IV. CONCLUSION

As the insider having the credentials it is easy for them to break the system and harm the system. There are different criteria for understanding the threats based on how they are harmful to the system. Many detection criteria and methods are also explained. Each criteria provides understanding about the detection methods. Characterization and analyzing insider threats constitutes a major role in the detection methods. Many algorithms are described based on implementation, detection and risk analysis etc. Each algorithm having its own advantages and disadvantages. There is no methods which results a complete detection of these threats. Depends on the data sources, behaviors, and detection methods result varies. Using supervised algorithms C$4.5 algorithm, SVM, KNN, with same data source (Dynamic and static data) C4.5 algorithm produced better result for known attacks and SVM for unknown attacks. A comparison of supervised and unsupervised algorithms with SOM, Decision tree, HMM, SOM produces the high accurate detection and good visualization. Classification with behavioral data also provides different accuracies with each detection algorithms even with same data set. Hybrid methods always provides better results for detection. A combination of proper behavior models incorporation with statistical or machine learning models would provide better results. Current systems uses modeling the threats uses psychology, behaviors, and sociological behaviors separately. Human behaviors are also unpredictable. As an advanced level, it is good to understand the stages of insider intrusion, analyses them and use combination of behavioral and conventional models and multiple detections methods can be used.

REFERENCES

1. Jennifer U Mills, Steven M F Stuban, Jason Dever "Predict insider threats Using Human behaviours" in IEEE Engineering Management Review, Vol-45, No.1 First quarter 2017
2. Anton, S., I. SimonaTUTUIANU. 2015. The complex and dynamic nature of the security environment. Proc. International Scientific Conf. Strategies XXI.
3. Bensing, R. G. 2009. An Assessment of Vulnerabilities for Ship-based Control Systems Naval Postgraduate School, Monterey, CA.
4. M. Bhuyan, D. Bhattacharyya, and J. Kalita, "Network anomaly detection: Methods, systems and tools," IEEE Commun. Surv. Tuts., vol. 16, no. 1, pp. 303–336, First Quart. 2014.
5. M. Bishop, D. Gollmann, J. Hunker, and C. W. Probst, "Countering insider threats," in Dagstuhl Seminar Proceedings 08302, 2008, pp. 1–18
6. Mouna Jouini, Latifa Ben Arfa Rabai, Anis Ben Aissa,"Classification of insider threats in information security system", 5th International Conference on Ambient systems, Networks and Technologies.Procedea Computer science 32(2014) 489-496
7. "Threat Modeling in Security Architecture – The Nature of Threats", Lukas Ruf, Consecom AG, Anthony Thorn, ATSS GmbH, Tobias Christen, Zürich Financial Services AG, Beatrice Gruber, Credit Suisse AG, Roland Portmann, Hochschule Luzern ISSS working group of society architecture
8. Swiderski F, Snyder W,"Threat modeling", Microsoft press, 2004
9. Liu Liu1, Olivier De Vel2, Qing-Long Han1, Jun Zhang1, and Yang Xiang1," Detecting and Preventing Cyber Insider Threats: A Survey", IEEE COMMUNICATIONS SURVEY & TUTORIALS-2018
10. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM computing surveys (CSUR), vol. 41, no. 3, p. 15, 2009.
11. Kandias, A. Mylonas, N. Virvilis, M. Theoharidou, and D. Gritzalis, "An insider threat prediction model," in International Conference on Trust, Privacy and Security in Digital Business. Springer, 2010, pp. 26–37.
12. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligencedriven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," Leading Issues in Information Warfare & Security Research, vol. 1, p. 80, 2011.
13. Dinil Mon Divakaran, "Insider threat detection and its future directions", Article in International Journal of Security and Networks · December 2016
14. Cappelli, A. Moore, R. Trzeciak, and T. J. Shimeall, "Common sense guide to prevention and detection of insider threats 3rd edition–version 3.1," CERT, Software Engineering Institute, Carnegie Mellon University, Tech. Rep., 2009
15. Cappelli, A. P. Moore, and R. Trzeciak, "The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes, 1st ed. Addison-Wesley Professional, 2012.
16. CERT Insider Threat Team, "Unintentional Insider Threats: Social Engineering," Carnegie Mellon Univ, vol. CMU/SEI-20, no. January, 2014.
17. Duncan, S. Creese, and M. Goldsmith, "An overview of insider attacks in cloud computing," Concurr. Comput. Pract. Exp., 2014
18. Antonia Nisioti, Alexios Mylonas, Member, IEEE, Paul D.Yoo, Senior Member, IEEE, Vasilios Katos, Member, IEEE From Intrusion Detection to Attacker Attribution: A Comprehensive Survey of Unsupervised MethodsIEEE survey and tutorials,2018
19. DETECTION, I. (2002). Intrusion detection: a brief history and overview.
20. Laskov, P., Düssel, P., Schäfer, C., & Rieck, K. (2005, September). Learning intrusion detection: supervised or unsupervised?. In International Conference on Image Analysis

and Processing (pp. 50-57). Springer Berlin Heidelberg.
21. "Insider Threat Detection Using Graph-Based Approaches", William Eberle Lawrence Holder, Cyber security Applications & Technology Conference For Homeland Security,IEEE2009
22. Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2016). A multi-step outlier-based anomaly detection approach to network-wide traffic. Information Sciences, 348, 243-271.
23. Kim, Gisung, Seungmin Lee, and Sehun Kim. "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection." Expert Systems with Applications 41.4 (2014): 1690-1700.
24. "A Hybrid Network Intrusion Detection Technique Using Random Forests", Jiong Zhang, Mohammad Zulkernine,ARES '06 Proceedings of the First international conference on Availability, Reliability and security,IEEE Computer security Society Washington,DC,USA,2006
25. 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
26. A. E. Ahmed and I. Traore, "Anomaly intrusion detection based on biometrics," in Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop. IEEE, 2005, pp. 452–453.
27. Y. Song, M. B. Salem, S. Hershkop, and S. J. Stolfo, "System level user behavior biometrics using fisher features and Gaussian mixture models," in Security and Privacy Workshops (SPW). IEEE, 2013, pp. 52–59.
28. J. Zhang, Y. Xiang, Y. Wang, W. Zhou, Y. Xiang, and Y. Guan, "Network traffic classification using correlation information," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 104–117, 2013
29. A. Tuor, S. Kaplan, B. Hutchinson, N. Nichols, and S. Robinson, "Deep learning for unsupervised insider threat detection in structured cyber security data streams," in AI for Cyber security Workshop at AAAI, 2017
30. M. Hanley and J. Montelibano, "Insider threat control: Using centralized logging to detect data exfiltration near insider termination," DTIC Document, Tech. Rep., 2011
31. IElise T Axelrad,Paul J.Sticha,Oliver Brdiczka,Jianqiang Shen"A Bayesian network model for predicting insider threats,"IEEE security and privacy workshop,2013
32. Ameya Zanzgiri, DipankarDasgupta, "Classification of Insider Threat Detection Technique" Conference'CISR'16, April 5–7, 2016, Oak Ridge, TN, USA. Copyright 2016 ACM
33. Hastie, T., Tibshirani, R., and Friedman, J. 2008, The Elements of Statistical Learning (2nd edition). SpringerVerlag
34. Ted E. Senator, Henry G. Goldberg, Alex Memory" Detecting Insider Threats in a Real Corporate Database of Computer Usage Activity"ACM, 2013
35. L. Spitzner, "Honeypots: catching the insider threat," 19th Annu. Comput. Secur. Appl. Conf., no. Acsac, 2003
36. Abdul Aziz Almehmadi, Khalil-El-Khatib, "On the Possibility of Insider Threat Detection Using Physiological Signal Monitoring"SIN'14 Proceedings of the 7th International Conference on Security of Information and Networks

AUTHORS PROFILE

Lekshmipriya S B Completed B tech from University College of Engineering, Thiruvananthapuram, Kerala and M E from St.Peters University, Avadi, Chennai. Currently designated as Research scholar in Jerusalem College of Engineering, Chennai, working in the area of cyber security.

Dr.G. Geetha received her B.E computer Science and Engineering from Bharathiar University, Erode in 2000, M E computer Science and engineering from Sathayabama University, Chennai in 2005 and PhD from Anna University, Chennai. Now she is working as professor in the department of Computer Science and Engineering at Jerusalem College of Engineering, Chennai. She has 15 years of teaching experience. Her area of interest includes Network Security, Software agents and Mobile Security. She is recognized as supervisor for guiding PhD Research scholars of Anna University and produced 3 doctorates 2016.