Journal of Applied Information Science
10 (1) 2022, 17-28
http://www.publishingindia.com/jais

Insider Threat Detection in Organization using Machine Learning

P. Varsha Suresh[1*] and Minu Lalitha Madhavu[2]
[1]Computer Science & Engineering, Sree Buddha College of Engineering, Pattoor, Kerala, India.
Email: varsha2361995@gmail.com
[2]Computer Science & Engineering, Sree Buddha College of Engineering, Pattoor, Kerala, India.
Email: minulalitha@gmail.com
*Corresponding Author

Abstract: A Cyber Attack is a sudden attempt launched by cybercriminals against multiple computers or networks. According to evolution of cyber space, insider attack is the most serious attack faced by end users, all over the world. Insiders that perform attack have certain advantage over other attack since they familiar system policies and procedures. It is performed by authorized person such as current working employee, pre-working employee and business organizations. Cyber security reports show that both US federal Agency as well as different organizations faces insider threat. Compromised Users, Careless Users and Malicious Users are some of the ground for insider attack. User-Centric insider threat detection based on data granularity provide a new extent for insider detection since data is analysed on it's depth. but, improper selection of feature is a demerit. As a result, Data granularity with two stage confirmation method is used in the proposed system. In the first stage dual filtering using Hidden Markov model and fuzzy logic is involved. In the second stage, the predicted output from first stage is again checked using profile-to-profile or template-to-template comparison. The selection of user's information as well as triple feature for generating training set is an additional advantage of the proposed approach. Two stage confirmation leads to increase in performance measure with very low false positive rate.

Keywords: Cyber security, Fuzzy logic, Hidden Markov model, Machine Learning (ML).

I. Introduction

Securing information from unauthorized access is known as Information Security. The practice of stopping the disclosure, disruption, modification, inspection and destruction of information without knowledge of user. Information can be anything like user's details, profile on social media, data in mobile phone or biometrics etc. Authentication and authorization are essence of information security. Authentication does the duty of confirming a person's identity while authorization does the work of providing appropriate privileges to an individual after verifying the person's identity. Cyber Security is the approach of technologies to check and to safeguard systems, networks, devices and data from cyber attacks. A cyber attack can illegally damage computers, steal data, or use a breached computer as a starting point for other attacks. Cyber Security is the state of safeguarding and recovering computer system from any type of cyber attack. Cyber attack can be divided in to insider as well as outsider attack. There are different types of cyber attack such as Phishing, Man in-the-middle attack, Denial-of-service attack etc. According to the evolution of cyber space Insider attack is the most promising attack faced by user's in today's world. A threat that originates inside the industry or government firms, and causes exploitation is known as internal Cyber threat or internal cyber attack. Insiders that perform attacks have a dominance over external attackers because they have approved system access and also may be familiar with web architecture and system guidelines. Moreover, there may be fewer safety against internal cyber attacks because many firm focal point is on protection from exterior attacks. As claimed by Clearswift Insider Threat Index (CITI) [25] annual report 74% of data security breaches in past 12 months were originated by insiders. Source of attack or behavior of attack are used to classify security attack. Source defines the place from which attack originate and behavior defines the aggressive behavior which leads to forceful access of data. Attacks are classified as insider or external attack in case of the former and in the case of the latter, they are classified as active or passive attacks. External attack originate from the outside the organization and some of the important external attack are network security attacks, physical security attacks, etc. A malicious attack caused by an individual within the organization is known as insider. Insider may be a current working employee, a former employee or a business associate. Whereas, Active attack has more importance over passive attack as it tries to modify the content of the messages. In case of Passive attack, an attacker observes the messages or it's content and subsequent retransmission takes place.

According to cyber security report, 25% of all the attacks to organizations are due to insider and their number is increasing day by day. It is very much importance in the current era.

According to recently published report of IBM, because of COVID-19, 53% of employees are working from their home using personal laptops and 61% employees haven't provide tools to properly secure those devices, which leads to loss of secure data and it is done by a known person. Actually insider threats have been an issue for companies long back, but they have gain more strength after the system gotten increasingly interconnected. The study sponsored by Ponemon Institute which was sponsored by IBM explains that insider-related incidents costs $4.3 million in year 2016. According 2018, cost for these internal cyber attacks was $8.7 million. This is the big take away and the data breach cost is trending upwards both in the US as well as globally. In 2019 also the number of attacker is increasing tremendously, which leads to increasing in lose that was faced by organization. Same time user's or each individual may effected by insider attack or an internal friend who behave as an attacker. User's personal information or credentials are traced by the attacker without the knowledge of user. As a result, the user may also face many problems such as lose of money or their personal properties etc. Different techniques are introduced prevent insider and their harmful attack.

The objective of this paper is to understanding the harmful effect of internal cyber attack. The lose which is faced by individual or organization over years. Analysing different work to understand the move made by an insider. Understanding what are the different methods used by business organization to prevent insider before attack takes places. To propose a new and advance techniques to detect insider and reduces the harmful effect. To bring forward a novel two stage confirmation techniques to protect from insiders.

The important contributions of this paper are outline as follows:

- We first give a brief idea of the Cyber Security, followed by providing knowledge about insider as well as outsider attack.
- We provide information about different type of insiders which exist in the organization.
- We present a novel approach using two stage confirmations to protect from internal cyber attack.
- We mention the use of two important machine learning algorithm that is fuzzy and Markov model.
- We bring the use of the concept anomaly based detection and misuse detection in the second stage of confirmation.
- We mention the advantage of data granularity and proper selection of user's information and triple features for detection of insider.
- Finally, we illustrate a theoretical analysis between the existing and the proposed insider detection models.

The remainder of the paper is Section II describes the Method of Study. Section III provides an overview of Insider Cyber Attack. Section IV describes the related works explaining different insider detection techniques. Section V explains the proposed insider attack detection method. Section VI illustrates the theoretical analysis performed between the existing and the proposed insider detection models. Section VII concludes the paper and provides future directions.

II. Method of Study

This paper proposes a novel approach for insider detection using two stage confirmations. The objective is to propose a new approach which tackles the problem in the existing approach and improves the efficiency. The reviewed papers concentrate on diverse task which have been considered to study the negative effect of insider attack (Internal Cyber attack) to organization such as lose in money, reputation and secret files and data of companies. The findings of these works are very effective on learning the issues and increasing estimate to address solution. We spend most of time to explore different facts such as Taylor and Francis, Elsevier, Science Direct, Springer, IEEE Explore, and other computer science journals and conference. In searching sentences and keywords we used application of cyber security in organization and government agencies. We inspect each and every article's reference list to recognize any potentially applicable research or journal title. The publication period taken into consideration is 2010 to 2021. For exploring different we collect abstract and keywords of PDF, reports, documents and full length paper. Furthermore, in searching different information for getting content we used journal, conferences paper, workshop papers, topics related publication, expert lectures by expert or talks and other topic related communities such as Overview of insider attack, Insider attack challenge to organization, Insider and Outsider Data Security threats. Different video and lecture class related to the harmful effect of insider, paved the way for research work. Different review and research paper on reputed journal enable us to understand the demerit of existing system and drawback of proper selection of feature. So, for this research, we collect information from two sources and take the application of machine learning to do this research with all sincerity.

III. Overview of Insider Attack

Attack that originates inside the industry or government firms, and causes exploitation is known as Internal Cyber Threat or Internal Cyber Attack. Insiders have dominance over external attackers because they have permitted system access and also are familiar with the architecture of network as well as system procedures. Moreover, it has less security against insider attacks when compared with external attack.

Types of Insider Attack are:

- *Malicious Insider*: A Turncloak, who maliciously and intentionally abuses credentials such as Password, to steal information for financial or personal reason.
- *Careless Insider*: An innocent user who unknowingly reveal the system to outside threats. It is common type of

insider threat that arises from mistakes, such as keeping a device expose. Careless insider may arises when an employee unknowingly click an insecure link, affecting the system with malware.

- *A Mole*: A person who is actually an outsider but behave as an insider to gain access to a privileged network. Actually the outsider impersonate as a worker in the organization.

An insider threat is one of the most expensive types of attacks and hardest to detect. It mainly occurs inside the organization by peer worker or colleague with our knowledge. An employ change in to insider due to dissatisfaction in his work. Due to avoidance of promotion or unnecessary cutting of income will change their mind. Sometimes, company may not provide employee proper reward or sudden termination may lead the path to an insider. This circumstance of worker is usually used by other agencies to make him insider. Most probably legible user becomes insider because negative effect environment in which they live.

IV. Related Works

Insider attack is a cyber attack performed by authorized person such as current working employee, pre-working employee or business organization. Insider or Internal Cyber attack detection system proposed by several authors and their merits along with demerits on it's detection and prevention are discussed in the following sections:

A. Insider Attacks at SC Level by using Data Mining and Forensic Techniques

Computer systems select user IDs and passwords as the login credentials to authenticate users. Mostly, login patterns are shared by the individuals with the co-workers and request them to assist co-tasks. As a result, safety of pattern used is not up to the mark. A legitimate users of a system who perform malicious action to the system internally, are difficult to determine as intrusion detection systems and firewalls detect and destroy harmful action occurs from outside the system. Fang-Yie Leu *et al.* [1] propose a system, named Internal Intrusion Detection and Protection System (IIDPS), to identify insider or internal threat at system call (SC) level by mining the data as well as using forensic features. The IIDPS determine login user is a account holder by comparing with the users' personal profiles. User's usage habit is used as forensic feature for the detection purpose. The IIDPS is organized by distinct element such as System call monitor and filter, two type of server such mining and as well as detection server, grid for computation purpose, and three repositories are also used such as log files of user, profiles of user and attacker. The SC monitor and filter gather SCs submitted to the kernel and save these SCs in a format which consist of user ID, the process ID, and the SC passed by the users. User's input is stored in user's log file. The mining server check the log data with data mining techniques to understand the user's computer usage habits, which are then stored in the user profile. The detection server makes a comparison between users' behavior patterns with those SC-patterns gathered in the attacker profile and those in user profiles to detect harmful behaviors and attacker. When an intrusion is identified, the detection server alert the SC monitor and filter to separate the harmful user from the protected system. The purpose is to ban the user from continuously attacking the system.

Ability of identifying and preventing attack has been analyzed in this paper. This has been done by means of a experimental testbed, which consists of 12 users to verify the feasibility and accuracy of the IIDPS and the results shows that mining of information as well as historic feature are used for intrusion detection provide strong resistance against threat. The results also demonstrate that IIDPS can effectively prevent different aforementioned attacks. Detection and mining speed of approach is high. Similarity scores in this approach helps to identify unknown user accurately. Accuracy of detection of attack in IIDPS is 94.29%, and the response time is less than 0.45s means it can prevent protected system from insider attacks effectively and efficiently. IIDPS pay out 0.45s to spot a user. The demerits bounded with data mining and forensic technique is that third-party shell command is not used in this approach to improve the system performance. IIDPS may detect inaccurately when user's habit suddenly changes.

B. Insider Attacks Detection in Big Data Systems

Big Data is a gathering of information that is vast in volume, which is raising exponentially. It is an area with so large size and complexity that none of data management tools can process it efficiently. In such a System Information Security is a major opposition for Big Data System. From a customer point of view one of the main risks in adopting big data systems is in trusting the provider who protects the information. Santosh Aditham *et al.* [2] propose new system architecture in which insider or internal cyber attacks can be identified by using the replication of information on different nodes in the system. It utilizes a two-step threat detection algorithm and a safe communication protocol to identify processes running in the system. At most two step in which construction of control instruction is the first step and second step involves their matching. The first and foremost step in the attack detection is process profiling, which is conducted independently at each and every node to identify different attacks and the second step is hash matching which is performed by replica data nodes understand about the legitimacy of attack. It is a combination of independent security modules that work simultaneously and reside on individual nodes of the system. Information transferred between the safety elements in the system architecture contains meaningful knowledge about the analysis of a process. Hence, a public key cryptosystem is used for secure communication. All information transferred by node using secure communication channel is encrypted by

using private key and copies of the keys are not available to anyone. The associated public key will be passed with all other duplicate nodes that an information node needs to communicate. Actually the proposed security system is a combination of 3 parts that is secure communication protocol, process profiling and hash matching. The three parts are formed of different modules that need to be installed in to big data system. Secure communication protocol is used to send, receives or queue message. Process profiling is used analyze as well as encrypt data. Verification and consensus is used to decrypt, verify and notify about attack.

Different method used to increase the privacy and security of data in Big Data System. Mean while, providing a positive vibe to user who trusts Big Data. Techniques used to prevent insider has been discussed in this paper. This has done by means of real-world hadoop and spark tests indicate that the system needs to consider only 20% of the code to understand a program and suffers 3.28% time overhead and the result shows that the security system can be built for any big data system due to its external workflow.

The results also demonstrate that the system detect insider attacks quickly with low overhead. It aims to provide robust security for big data systems. The limitation associated with this approach is that need to provide methods to evaluate system on security related benchmarks. Also, lack of commencing hardware architecture of security chips that can support the system.

C. Selective Jamming/Dropping Insider Attacks in Wireless Mesh Networks

Wireless mesh networks promise to extend high-speed wireless connectivity beyond what is possible with the current WiFi-based infrastructure. However, their unique architectural features leave them particularly vulnerable to security threats. Loukas Lazos *et al.* [3] say that unlocked nature of the wireless channel leaves it to jamming attacks. Anti-jamming method includes some type of spread spectrum (SS) communication, in which the signal is passed across a large bandwidth according to a pseudo-noise (PN) code. SS can protect the wireless communications safe to make PN codes secret. If an insider has the knowledge of the commonly shared PN codes can still make a jamming attack. WMNs are a combination of two-tier network architecture. The first tier incorporate end users, they are also known as stations (STAs), which is merged with mesh nodes, and known as mesh access points (MAPs). The second tier or stage is made of a peer-to-peer interconnections of the MAPs. Connectivity in the second tier is supported by mid-way routers known as mesh points (MPs), which connect MAPs (MPs do not receive interrelation from end users). The interconnection of MAPs and MPs is usually static in nature, and use different frequency bands to transmit data and control information. Finally, mesh gateways (MGs) support connectivity to the wired infrastructure. Internal attacks or Insider attack, which are begin from compromised nodes, are much more knowledgeable in nature. These attacks uses ideas of secrets of networks and protocol to carefully and secretly target critical network. Internal attacks, also known as insider attacks, cannot only prevent using energetic methods that focus on network secrets, because the attackers already have an idea. If selective jamming is not effective due to anti-jamming measures, an insider can carefully drop packets. Once a packet has been accessed, the compromised node can audit the packet headers, classify the packet, and think whether to pass it or not. Such an action is often termed misbehavior. Post-reception dropping is less tensile than selective jamming because the adversary is minimal to dropping only the packets routed through it.

Ability of selective Jamming or Dropping insider attack in Wireless mesh network has been analyzed in this paper. The results also demonstrate that to it helps to avoid the use of common secrets for protecting broadcast communications. Limitation bound with approach is that heightened tier of security comes at the expense of performance. Other one is accurate behavioral monitoring mechanisms that do not depend on continuous overhearing, and proper maintenance and dissemination of reputation metrics.

D. Geo-Social Insider Threat Resilient Access Control Framework (G-SIR)

The most dangerous and costly threat to institutions is denoted as Insiders. These attacks are carried out by user or person who has authorized access to the system. Preventing insider attacks is a discouraging task. Nathalie Baracaldo *et al.* [4] propose Framework G-SIR to deter insider threats by including current and historic geo-social knowledge as part of the entrance prevention decision process. By analyzing users' geo-social behavior, insider can be those users whose access behavior varies from the normal patterns, such anonymous character can lead to potential insider attackers who may intentionally carry out harmful activities. Such information to determine how ethical a user before granting access. The proposed system consist of AC guideline specification and enforcement strategy designed to understand users' geo-social behavior. The AC component collects present and historic geo-social interactions to predict whether an access should be granted or denied. A role may have a spatial scope that specifies particular locations where it can be activated by users assigned to it. Geo-social constraints indicate area that users assigned to the constrained role cannot visit and user they cannot frequently meet. Vicinity constraints force a restriction on individual that may or may not be at a particular distance from the requester at the time of an access. Mainly there are two types of vicinity constraints such as inhibiting and enabling constraints. Inhibiting constraints gives the idea that permission needs to be denied, if inhibiting

users are identified in the vicinity. Enabling constraints are used to understand the importance of permission in the vicinity of the requester. Geo-social trace based constraints are constraints that a user to go after a certain geo-social path before they can be authorized to access a particular resource. Geo-social obligations are geo-social actions that users need to manage after they have been granted permission. All monitoring and likelihood computations described take place in the Monitoring, Context and Inference Module. It specifies the context of a user, which contain information such as the current device used by the individual, type of connection used, etc. The Access Control Module is in charge of creating AC decisions.

Ability of identifying and preventing attack in G-SIR has been proposed in this paper. This has been done means of a distinct indoor simulator carried out in Java and the results indicate that this is the first and foremost effort to use geo-social information to deter insider threats by integrating it into the AC mechanism.

The results also demonstrate G-SIR is efficient, scalable and effective to detect insider by including historic and geo-social knowledge. It contains various geo-social constraints and enforcing these conditions helps to minimize the risk of proximity, social engineering and probing threats. The limitation bound with this approach is that behavioral knowledge should be considered at the time AC decisions. However, designing a system that uses such information without expanding the risk exposure is a challenging task.

E. Addressing the DAO Insider Attack in RPL's Internet of Things Networks

In RPL routing protocol DAO which is a information used for control are passed by the child nodes to their corresponding parents to produce descending routes. A harmful insider node can utilize these characteristics to send fraud DAOs to its parents periodically, activate those parents to pass the fake messages to the root node. These characteristics can have a harmful side effect on the production of the network, power consumption can be increased drastically, latency, and reliability can be reduce to an extent.

RPL arrange its physical network into a shape of Directed Acyclic Graphs (DAGs), If DAG is implant at a single destination, then it is known as a Destination-Oriented DAG (DODAG). To incorporate traffic pattern to upward, DODAG should be constructed, topology centered at network root. The manufacturing of the DODAG launch with the root multi-casting control messages called DODAG Information Objects (DIOs) that is passed to RPLs neighbors. Baraq Ghaleb *et al.* [5] demonstrate RPL node as a available stopping place from the root. An important reality of transferring a DAO message by a child node will leads to passing of many copies of DAOs that is equivalent to the number of intermediate parent nodes. An oponent can utilize this information to harm other network continuously transmitting DAOs to its parent node. In order to determine a DAO internal attack in RPL, a new approach called SecRPL is used, that prevent the count of forwarded DAOs by a parent. In fact, there are two opinion for applying this restriction. Former is to regulate the total count of transmitted DAOs regardless of the source node, the second is to prevent the count of transmitted DAO per destination. Second option is better compared to previous option and result in preventing some DAOs coming from non malicious junction or node. It may also leads to block DAOs of some nodes and no effect to some others DAO. In addition, parent node maintain a counter with each child node in its sub-DODAG. In case, if the number of forwarded DAOs exceeds threshold value, the parent discards any DAO message. It also make clear that no node will be blocked due to the time factor, after two consecutive DIOs, counter is reset. Mainly, when the parent node passes a DIO message, all child node counters are reset.

F. Securing Wireless Medium Access Control Against Insider Denial-of-Service Attacks

An malicious user (attacker) who default the network can start more harmful denial-of-service (DoS) attacks than a External user by passing large amount reservation requests to block the bandwidth.

Secure MAC is an approach used to protect against such insider threats. It consist of four components such as channelization which is used to block large reservations, randomization method is used to counter reactive targeted jamming, coordination perform duty to prevent control message aware jamming and again over reserved and under-reserved spectrum should be solved and assignment of power to find out each node's contribution to the particular power. Sang-Yoon Chang *et al.* [6] demonstrate a general handshake-based MAC framework where it denote how to send a packet, how the transmitter shows a MAC-layer decision based on its observations and the knowledge from previous transmission rounds. Save as well as reserve the channels for data transmission. Reserved channels are used for transmission of data packets and feedback is gain from the receiver as well as the network.

In wireless MAC, an internal attacker can carry out the following actions that are more damaging than those from external users. False reservation injection means holding the channel resources without operating them, false feedback distribution consist of announcing wrong data to twist the action on MAC control to the attacker's favor, and MAC- aware jamming where jamming is based up on to the received control messages. False reservation hide bandwidth to actual users and takes small insider resources and use network resources out of proportion to attacker effort, it is more efficient mistake than jamming. The goal of channelization is to distribute spectrum bandwidth to each user proportional according to their power capability, guarantee a specific power spectral density. Channelization

actions are made only once per round. The coordination solve these problems by enhancing the bandwidth allocation and the randomization output solving certain conflicting reservations and sharing transmission to area that would otherwise be not utilized. Finally, after each round of information transmission is over, each junction carryout power attribution to calculate the count of power contributed for communication of data by each node.

G. Securing VPN from Insider Bandwidth Flooding Attack

The insider attack is launched by users residing within the trusted zone of the VPN site. They are the legitimate users of the VPN service. Flooding packets are used for easily attacking the VPN service. Safeguarding from insider or internal cyber attack is more difficult then external cyber attack as it is launched by users who have authorized access to the VPN service. This type of flooding attack disrupts the VPN service to its other legitimate users. Network security deals on safeguarding network perimeter from outside threat even though internal attack is more serious. It's aim is to add a control mechanism for bandwidth to control the bandwidth each individual. The bandwidth control mechanism must ensure that the packet through the reserved bandwidth is within the allowable limit. Control mechanism has used to reduce dropping packets from the flooding source which protect authorized user from harmful attack. Saraswathi Shunmuganthan *et al.* [7] describes Virtual Private Network (VPN) is an encrypted connection over Internet from a device to a network. It helps to transmit data from a branch office to main office. Flooding is a routing algorithm present in computer network in which all arriving packet is passed through every other link not on the link from which it has came.

VPN site 1 and VPN site 2, are connected to gateway routers called customer edge (CE). CE1 and CE2 are interconnected to provider edge (PE) routers PE1 and PE2. Bandwidth is actually maximum data transfer rate over network. Customer Edge router ensures that bandwidth allocated to VPN site is being fairly distributed among users to avoid insider attack. It employs entropy based probabilistic model at CE router to rate limit of insider attack traffic. Entropy is used to measure the uncertainty. Entropy is used to calculate deviation of user from normal use age.

H. Insider Threat Risk Prediction based on Bayesian Network

Bayesian network is a graphical model based on probability, consist of a number of variables via directed acylic graph (DAG) is used to show conditional dependencies. Nebrase Elmrabit *et al.* [8] demonstrate that the features which used by the graph are technological aspects, Organizational impact and Human Factors. Information are collected from organization and particular measure sealing to ensure insider threat breaches are kept to minimum. Investment balance is the balance between investment in insider and outsider threat is key to understand insider threat breaches. Detection level is the measurement of how accurate detection system with regards to previous insider attack. Security and privacy control include forensic evidence, network as well as email logs. Organizational Impact is the information related to the way in which organization is structured and how insider threat breaches are managed. Organizational impact deals with information like security breaches, Structure, security policy as well as employee work-related stress symptoms.

Security breaches include breaches that have occured historically within the organization. Structure include information about recruitment procedure, previous employment screening. Security policy contain information related to organizational security policy. The fragile link in an information security chain is one and only human factors. It include motivation which include motivation for showing misbehavior, Opportunity is the factors which is available to perform attack. Capability includes the power to do something by the fellow being.

I. Motivation and Opportunity based Model

Situational crime prevention theory (SCPT) opportunities for misbehavior are lowered to an extent. Social Bond Theory (SBT) can be used to help understand motivation to engage in misbehavior. Raise in effort, risk and lower the rewards, stimulation, keep away exempt are the elements considered in SCPT. Nader Sohrabi Safaa *et al.* [9] explains SBT pivot on mainly four factors such as organization attachment, relation with institution or organizational, involve n a particular work, and personal standard. Increase the effort is used to raise the amount of effort which is taken to perform attack. Increase the risk is used to increase amount of risk that is faced by the attacker, when he/she do a malicious action which is harmful to organization. It also reduce the excuse which made by worker in doing mistake, since they fear to do it again. Reward which the attacker gets by doing mistake is also reduce drastically.

Social bond theory includes attachment with the organization. If there is any problem with the organization as well as worker, chance of performing attack is more. Commitment with the organization is also considered. If a person is commitment with organization, he/she will not do any negative thing to the organization. Workers involvement with the organization show that whether he is an attacker or normal user. If user is sensitive towards organization, he/she will not do any malicious activity.

J. User Behavior Modeling and Anomaly Detection Algorithms for Insider Detection

Junhong Kim *et al.* [10] demonstatre user behavior-modeling phase, where each user's behaviors are converted in to daily activity summary, e-mail contents, and e-mail communication network. Anomaly detection algorithm consist of Gaussian density estimation (Gauss), Parzen window density estimation (Parzen), principal component analysis (PCA) and K-means clustering (KMC) are algorithms used for separation of pattern. Gaussian density estimation which is important anomaly detection algorithm is used exhibit probability distribution of variable which distributed randomly. Parzen window classification is used for density estimation. It finds a point of interest. Only the features inside the window are considered to find which group the point of interest is present. It is used to calculate output probability when a point is given. Principal component analysis is used in dimensionality reduction for the reduction of noise or unwanted data. Dimensional Reduction consists of feature selection and feature extraction. PCA comes under feature extraction in order to reduce noise or error. As the number of feature decreases, processing will be fast. K-mean clustering is an unsupervised algorithm does not have labeled data. Set of data is put together in a group or cluster. Cluster consists of object which is similar in nature. K denotes the number of cluster or group. For best classification of data in to different group, appropriate cluster need to find. The attack observation model surrender at most 53.67% of the detection rate by only tracking the top 1% of malicious or suspicious instances.

The papers [11], [12] propose many insider detection methods like alarm filters and Psychological model to predict malicious behavior.

V. Proposed System

Insider Detection techniques have been developed to protect the system from wide variety of internal attack performed by current working employee, Pre-working employee or Business Organization. It is used to safeguard the privileges, reputation, key documents and economics of the organization or institution. Several feature extraction techniques, Machine learning schemes, Psycho metrical and behaivour schemes are used to detect insider. But, due to lack of proper arrangement or proper capturing of data, this technique remains ineffective or the performance is not up to the mark.

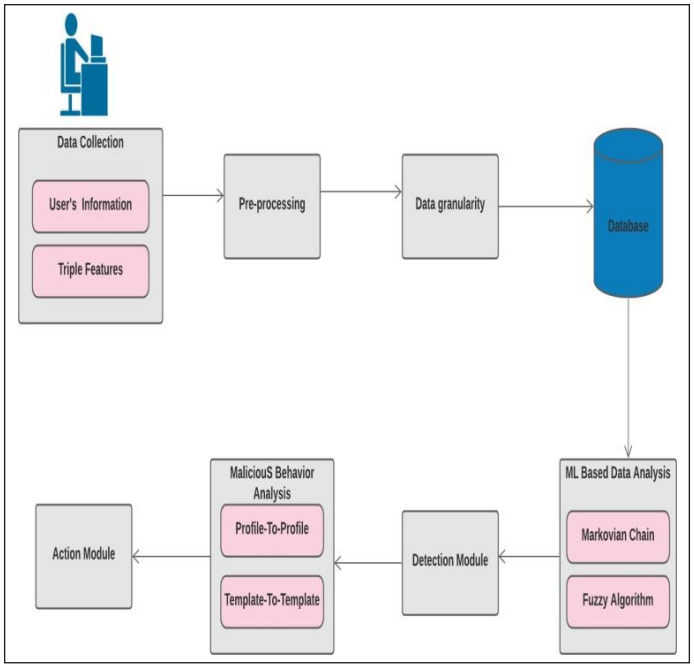

Fig. 1: Architecture of Insider Detection based on Two Stage Confirmation

Feature based decision modelling is required for identifying more attack. So, a novel insider threat detection method using two tier, fuzzy logic and Markov chain mechanism by collecting temporal feature, geographical feature and connection or re-connection feature is proposed.

The proposed system for malicious behavior and insider or internal cyber attack detection is shown in Fig 1. It has the following stages:

1. Data Collection: Data gathered from different sources are gathered and stored in a specified format. The two main categories are:
   - User's Information.
   - Triple features.
2. Pre-Processing: Identification of features and filtering of best features from the aggregated data occurs.
3. Data Granularity: Identification of collection of data segments is called granules.
4. ML Engine based Data Analysis: Two tier processing of data based on two important machine learning algorithm.
   - Fuzzy logic (FL) - Fuzzy Logic (FL) uses the method of human reasoning to derive a solution.

- Hidden Midden Model (HMM) - It is a machine learning model in which current state depend on previous state.

5. Detection Module: It is peculiarly for identification of insider from the organization.
6. Malicious Behavior Analysis or Behavior Analysis: This stage is primarily meant for the finalizing the insider as well as rejection of normal users.
7. Action Module: The insider who behaves as a normal user will face the consequences.

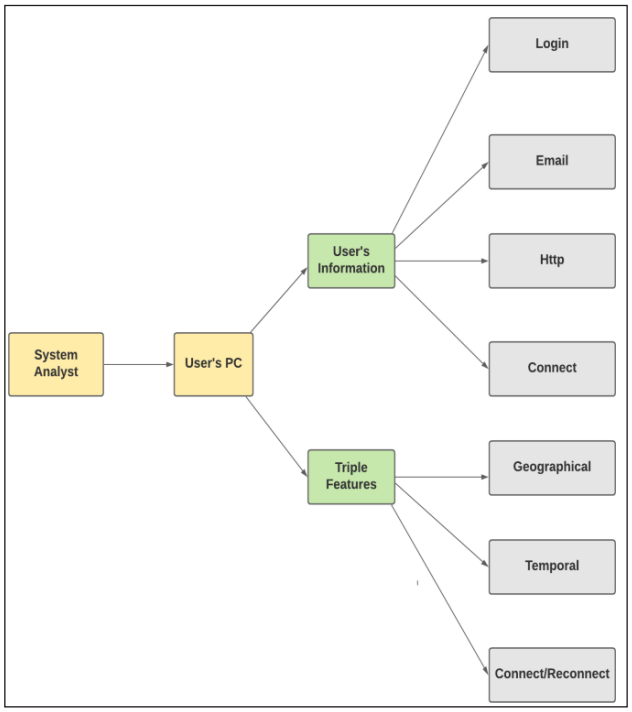

Fig. 2: Source of Data Collection

A. Data Collection

The entire system work based on the supervision of security analyst. A security analyst is a person who makes detailed studies to protect the system from unauthorized attack or cyber threat. The process of aggregation of data from different sources and their further processing is done by system analyst. A good observation method in connection with proper collection of data leads to successful application of ML techniques and also assist security analysts in making correct decisions. System analyst mainly concentrate on collecting information related to the user's daily action on work hours and after he working hours on the user's PC, shared PC and Websites. Fig. 2 represents the Data Collection process in proposed insider detection system. System analyst collect useful information for detection of insider from user's PC. They mainly concentrate on collecting two main categories of details. The User's information and Triple features. User's information mainly collected from Login, Http, Email and Connect features. They are Commo Separated file or .csv file. Triple features are mainly collected from geographical, Connect or Re-Connect features and Temporal features. These are three most important features which is used to detect insider. Hence, they are known as triple feature.

User's Information: User's Information is collected mainly from Login, Email, Http and Connect dataset. These are background data contain idea about user's motive or work within the organization. It gives a good idea about reality or abnormality of user's behavior. These are often actual data that need to be updated periodically. Since the user's behavior may change at any time. Above mentioned input dataset concentrate on the following contents:

- Http: It contains ID, date, action, PC and Url information.
- Here ID means MAC-ID is generally machine access identification. It is not similar to any machine. So, MAC-ID IS A unique name for identification of user's PC. Different PC has different MAC-ID. Date is actually the system date in which data transfer takes place. PC denote the number of PC which perform the operation. Action denote the specified action user perform. Url information stands for Uniform Resource Locator. It include domain name, with other detailed information to direct the browser to certain webpage
- Email: ID, date, pc, from, attachment, size and content, bcc and cc email address.
- ID means MAC-ID, Date is system date, PC denote the number of PC which perform the operation, From denote the from address, Attachment denote the count of details attached, Size denote the size of the file, Content indicate the details transferred, bcc indicate blind carbon copy allows the center of email to conceal the user's entered from bcc field from other recipients. CC means the actual carbon copy that is recipient can see to whom all this message has been send.
- Login: ID, date, pc and activity.
- ID means MAC-ID, date is the same system date, PC is the PC number, and activity indicates the login and log off phenomenon.
- Connect: ID, date, user, pc, activity. ID the MAC-ID, date is the same system date, user indicates the user name, pc indicates the pc number and activity indicate how many time the user connect or disconnect.
- Triple Features: Triple features means the three main features which contribute for insider detection and provide and extra mileage for detection. These are moral real time features. By adopting these features, attackers can be analyze from depth.
- Geographical: It indicates the features of location, area or region. Here, longitude and latitude are considered. Black list area normally where the entries are blocked and not

considered. It contains elements that are not automatically possible to access a certain area.

- Temporal: Temporal feature helps to know the particular time in which attack has occurred. Time specification helps to know, which attacker logged in during the particular time. Since, it is an insider attack and it is performed by current working or pre-working employee of an organization or internal user, time specification helps to identify the internal attacker easily. It is based on time bound. Mainly to find time zone as well as time region.
- Connection or Disconnection States: Connection and re-connection phase count helps to know the arrival of attacker, when insider or internal user misbehave, disconnection occur, which helps to know the presence of abnormality. This will also contribute to the model building of threat profiles. It shows the indication of insider at particular moment. The effect of disconnection and reconnection states that to be logged in feature extraction module.

B, Pre-Processing

This stage actually delete non-continuous or records with no data. It identifies all the features properly and filters or select best feature based on relevant values. It actually enhances the "garbage in, garbage out" process of the system. Analyzing data carefully help to remove misleading results. It helps to improve the quality of data before running any analysis. DataSet with missing value lead to wrong results which can be removed by applying to pre-processing. If there are irrelevant, redundant, noisy and unreliable data, then knowledge discovery during the phase of training is more difficult. It increases the amount of processing time for preparation and filtering steps. Data preprocessing mainly includes cleaning, Instance selection, feature extraction and selection. The output of data preprocessing is the final training set.

C. Data Granularity

Identifiable collection of data segments is called granules. In a Dataset, certain field is combine to predict particular behavior. Such data is called granuled data. Data granularity is splitting or fragmenting data in to multiple pieces or granules report. The greater the granularity, the deeper the level of detail. Increased granularity can help you drill down on the details of each organization and assess its efficacy, efficiency. Different datasets contain login, http, email, content and triple features are combine to generate the granule data. Here granule data is the training data. User-centric insider threat detection based on data granularity provides an additional advantage to the proposed approach. It actually considering microscopic feature to break down data. Generally, Multiple Granularity means hierarchically breaking up the database into blocks which can be locked and can be track what need to lock and in what fashion. Such a hierarchy can be represented graphically as a tree.

Hierarchical representation of data granularity is shown in Fig. 3. Actually it's a tree, which is made of four levels of nodes. The highest level represents the entire dataset.

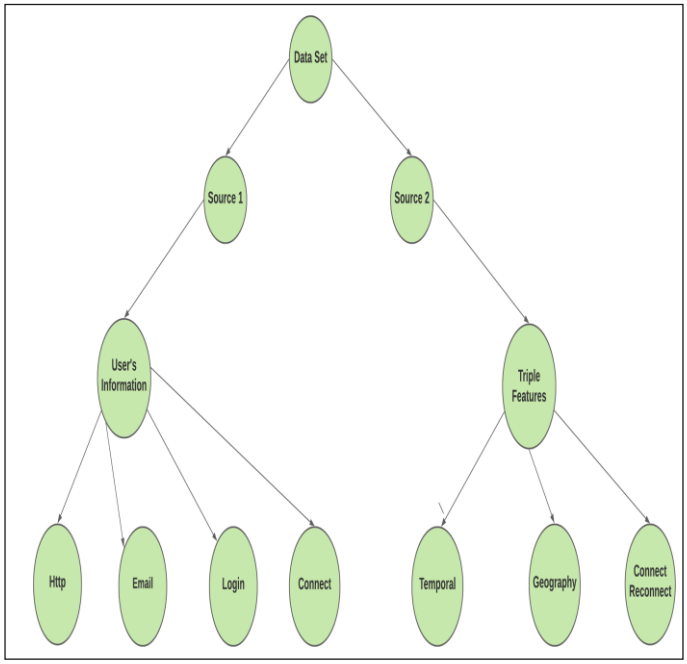

Fig. 3: Hierarchical Representation of Data Granularity

Below it are nodes of type source, which denote the source of information. The dataset consists of exactly these sources of information. Source 1 has child node which are called User's information. Source 2 has child node which is known as triple features. Finally, User's information has child nodes http, email, login and connect. Triple features have child nodes geographical, Connect or Reconnect, Temporal features. These are comma separated file and no file can be present in more than one Source of data. Hence, the levels starting from the top level are:

- Dataset.
- Source of Information namely source 1 and source 2.
- User's Information and Triple feature.
- Comma Separated files.

Example: User-Week, User-Day, User-Session are granule data of user's login information.

D. Machine Learning based Data Analysis

This stage uses machine learning based for the processing of data and detection of insider. Machine learning is from the knowledge that systems can grasp from data, understand patterns and make conclusion with reduced human intervention. Two stage filtering or two stage pruning is added advantage of this approach. Two important machine learning algorithm is used for this purpose. Hidden Markov Model (HMM) and Fuzzy Logic (FL). Microscopic level of detection take place in two phase detection, where two prominent algorithm of machine learning helps in accurately classify the data has attackers and normal user.

Fuzzy logic is used for handling combination of attribute. It is used for feature aggregation and reduction of feature. So, efficiency and speed of insider detection increases. Fuzzy logic is an important machine learning algorithm in which the real value of variables may be a real number which lies in between 0 and 1. It is working to use the partial truth concept, where value of truth varies between completely true and completely false. Fuzzy logic consider all possibilities and human way of decision making. If membership value of particular group is above a threshold then it is consider as important features for detecting insider. Attribute based comparison helps to know to insider at microscopic level. It helps to identify malicious user as well as malicious behavior. Fuzzy logic provides attention to Small false positive rate.

Hidden Markov Model (HMM), is assumed to be a Markov process. It moves through different state from the start state to end state. An important fact of Hidden Markov model is that current state depends on the previous state. The Markov process that is happening behind and hidden from rest of the world is actually Hidden Markov process. Here, based on this fact a person is considered insider based on the previous suspecting action. The action such as attaching multiple mails per second is a malicious or doubtful action. This hint is considered in next step for detecting insider.

Markov chain is used in first phase. Remaining condition which occurs is verified using fuzzy logic. This two-phase comparison helps to improve the accuracy of detection.

Fig. 4 illustrates the process in developing the proposed architecture. Initially the dataset of http, login, connect, email and triple features will be extracted from .csv file format as excel file by the data collection module. After pre-processing and filtering the best feature it is converted in to granule data. The granule data will be split as training and testing data. Two stage detection model use fuzzy and Markov is used to train the model with the training data. Once the model has been trained, the input data selected from the testing dataset will be given to the model. The model predict the MAC-ID of the insider as output. After generated MAC-ID, a second stage confirmation is done through Profile-to-Profile comparison or template-to-template comparison. Only after two stage confirmation, the final arrival in to the insider occurs. Based on that Alert or warning generated by the system analyst based on the decision of organization.

E. Detection Module

The MAC-ID generated by the fuzzy and Markov is passed to the detection. In detection module, the system actually recognize the insider from the organization. MAC-ID is unique ID. Each electronic device has their own MAC-ID. It is a unique identification code.

F. Malicious Behavior Analysis

This module actually enhances the efficiency of decision making process. An added advantage of Profile-to-Profile or template-to-template comparison occurs. Here, a two stage confirmation occurs. That is, it strength the decision which is made. Second level of comparison occurs in malicious behavior analysis.

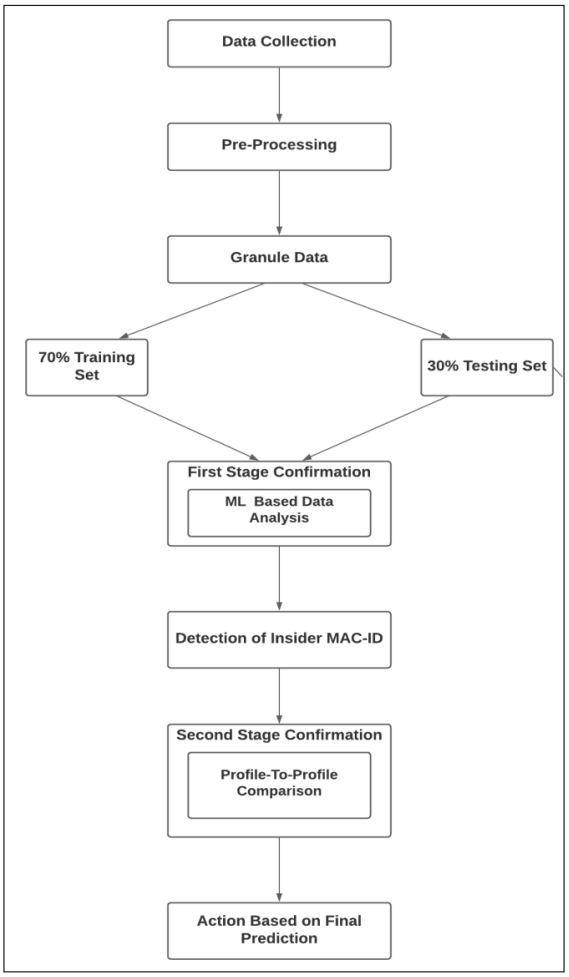

Fig. 4: Process of Insider Detection based on Two Stage Confirmations

Profile-to-Profile or Template-to-Template comparison, an automatic profile creation of attackers occurs. In Profile-to-Profile Comparison an automatic profile of employees is created in the database based on the day to day activities. It is a real time feature that gets updated periodically. In template-to-template comparison, a template of particular individual is already created based on some expectation that particular individual will behave in particular way. Actually it is already created expectation about an employee. It helps to identify insider easily. Here, a concept of misuse detection and anomaly detection is used. Misuse detection is actually signature based which can only detect known insiders by matching the features of incoming insiders with the historical knowledge and predefined rules. In case of anomaly detection automatically constructs a normal behavior of the insiders and detects incoming insiders by computing deviations. It can detect new insider which is not detected by two stage of pruning of fuzzy and Markov process.

Sudden change in user behavior can be identify using profile-to-profile or template-to-template comparison. Profile comparison help to identify attacker fastly and accurately. Using these features an automatic profile creating of attackers will help to identify them very easily.

After two stage confirmation by machine learning algorithm and profile-to-profile comparison the chance of false rate will be reduced tremendously.

G. Action Module

In action module system analyst analysis the prediction by machine learning algorithm and their performance measure. After two stage confirmation, final decision of insider occur. System Analyst compare the predicted MAC-ID with the original report and identify the employee who behave as an insider. They will forward the information with the organization. Based on the order from the organization system analyst generate alert, produce warning or blocking of certain url occur. For severe case, insider who behave as a legitimate user need to face suspension. For big lose, the insider will be sent to prison and entire gang of insider will be find out and protect the reputation and secret files of organization. Mean while, increase the trust of users.

VI. Theoretical Analysis on Insider Detection

A theoretical analysis on the existing and the proposed systems is performed. The existing mechanism implements only the psychometric and behavioral features and certain machine learning algorithm with proper collection of features to predict insiders, which leads to decrease in performance measures. But the proposed method implements two stage confirmation methods. The first stage uses novel method of detection using fuzzy logic and Markov features. It is a two stage filtering or pruning methods. Machine learning is an advanced and efficient technique than the existing ones. It builds an effective and highly accurate model than the existing behavioral based ones. The second stage of confirmation using profile-to-profile comparison helps to reduce false positive rate. The proposed model also uses user-centric insider threat detection using data granularity, which is efficient to develop accurate models than the existing ones. Data granularity is used for microscopic level of detection. Each small feature for detection of insider is considered with high importance. Since accuracy level is comparatively higher for the proposed system, efficiency will also be higher for the machine learning based insider detection models using two stage confirmations, when compared with the existing insider detection models. Selection of real time features such as temporal features, geographical and connection or re-connection features which is the triple features help to isolate the attack model. These type of genuine filtering method is absent in existing system which leads to increase the mileage of proposed system.

VII. Conclusion and Future Work

A insider detection model has been developed using novel approach of Fuzzy and Hidden Markov Model (HMM) for predicting the MAC-ID of insider in the organization. User-centric insider threat detection based on data granularity is important path for the detection of insider. Identical collection of data segments is called granules. It helps to drill down microscopic level of features for the detection of insiders. Two stage confirmation techniques is used. In the first confirmation stage, a two stage detection techniques using two important machine learning fuzzy and Markov improves the effectiveness of detection. Hidden Markov Model is used in the first stage and fuzzy is used in second stage. In the second stage of confirmation, profile-to-profile or template-to-template comparison. Two stage confirmation reduces false positive rate and based on the identification of insider, change in internal policy occur. Future scope of this work is that the Markov model cannot be true in estimating conditional probability between two states. The current work can be enhanced in the direction, so that the limitation of Markov analysis can be over-ridden. Modifying the existing Markov model with a fuzzy relation of attributes to a novel system that can predict the risk full outcomes from existing attribute is a new direction for the research.

Acknowledgement

This research was supported by Dr. K. Krishnakumar, the head of the institution. We would also like to show gratitude to the head of our institution, Dr. S. V. Annlin Jeba for sharing her pearls of wisdom with us during the course of research. We thank our colleagues from Sree Buddha College of Engineering who provided insight and expertise that greatly assisted us although they may not agree with all of the interpretations and conclusion of the paper.

References

[1] F.-Y. Leu, K.-L. Tsai, Y.-T. Hsiao, and C.-T. Yang, "An internal intrusion detection and protection system by using data mining and forensic techniques," *IEEE Systems Journal,* vol. 11, no. 2, pp. 427-438, 2015.

[2] S. Aditham, and N. Ranganathan, "A system architecture for the detection of insider attacks in big data systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 6, pp. 974-987, 2018.

[3] L. Lazos, and M. Krunz, "Selective jamming/dropping insider attacks in wireless mesh networks," *Electrical and Computer Engineering*, vol. 25, no. 1, pp. 30-34, 2011.

[4] N. Baracaldo, B. Palanisamy, and J. Joshi, "G-SIR: An insider attack resilient geo-social access control framework," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 1, pp. 84-98, 2019.

[5] B. Ghaleb, A. Al-Dubai, E. Ekonomou, M. Qasem, I. Romdhani, and L. Mackenzie, "Addressing the DAO insider attack in RPL's Internet of Thing," *IEEE Communications Letters*, vol. 23, no. 1, Jan. 2019.

[6] S.-Y. Chang, and Y.-C. Hu, "SecureMAC: Securing wireless medium access control against insider denial-of-service attacks," *IEEE Transactions on Mobile Computing*, vol. 16, no. 12, pp. 3527-3540, 2017.

[7] S. Shunmuganathan, R. D. Saravanan, and Y. Palanichamy, "Securing VPN from insider and outsider bandwidth flooding attack," *Microprocessors and Microsystems*, vol. 79, Nov. 2020, Art. no. 103279.

[8] N. Elmrabit, S.-H. Yang, L. Yang, and H. Zhou, "Insider threat risk prediction based on Bayesian network," *Computers & Security*, vol. 96, 2020, Art. no. 101908.

[9] N. S. Safa, C. Maple, T. Watsona, and R. V. Solms, "Motivation and opportunity based model to reduce information security insider threats in organisations," *Journal of Information Security and Applications*, vol. 40, pp. 247-257, 2018.

[10] T. Kim, Y.-S. Park, H. Cho, and J.-W. Kang, "Insider threat detection based on user behavior modeling and anomaly detection algorithms," *Appl. Sci*., vol. 9, no. 19, p. 4018, 2019.

[11] G. Yang, L. Cai, A. Yu, and D. Mengand, "A general and expandable insider threat detection system using baseline anomaly detection and scenario-driven alarm filters," *IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 2018.

[12] G. Yang, L. Cai, A. Yu, J. Ma, D. Meng, and Y. Wu, "Potential malicious insiders detection based on a comprehensive security psychological model," *2018 IEEE Fourth International Conference on Big Data Computing Service and Application (BigDataService)*, Bamberg, Germany, 26-29 Mar. 2018.