ISSN No:-2456-2165

Insider Attack Detection Implementation Using Behavior Analysis

Harshata Bhargava
Shri Shankaracharya Technical Campus
M.Tech Final Year Student
Dept. of Information & Technology
Bhilai, Chhattisgarh, India

Radhe Shyam Panda
Shri Shankaracharya Technical Campus
Head of Department
Dept. of Information & Technology
Bhilai, Chhattisgarh, India

Abstract:- Insider attack detection in an enterprise network environment is a critical problem that currently has no promising solution. This paper introduces new idea of use of sequence mining algorithms for distinguishing insider attack in network. According to current work we have discovered that mixes of pattern development with Behavior factors are most appropriate for recognizable proof of insider attack in any network. This paper presents experiments in which execution essentially helped in building an ideally estimated data structure representations of the sequence database that requires the need of Behavior parameters joining in insider attack identification calculations.

Keywords:- *Insider Attack, Network Attack, Data Mining Techniques, User Behaviour.*

I. INTRODUCTION

The issue of insider attack, likewise called insider misuse, includes a kind of computer security threat that has been considered for a long time. Early work by Anderson [1] depicts the nature of insider attack and classifies culprits of insider attacks into three gatherings: legitimate user, masqueraders, and clandestine users.

Masqueraders are users who get the login credentials of honest to goodness users and utilize these qualifications to despicably access endeavor applications and data. People delegated true blue users are the individuals who have authorized access to big business computing resources however who may misuse their access benefits to download extreme amounts of data or view data not required for playing out their job duties. At last, clandestine users increase authoritative access benefits past or even irrelevant to what they requirement for their job duties. Undercover users commonly known about the endeavor security systems and bypass those systems to access data. The arrangement talked about in this paper centers around detection of insider attacks by Masqueraders and legitimate users. [2] Gave a fascinating alternative method of characterizing and detecting insider misuse by considering the computing foundation level (e.g., network, system, and application levels) at which misuse can be recognized. Other broad earlier research has been conducted in the areas of systems, algorithms, and techniques for detecting insider misuse. An original paper by [3] builds up a model for a real-time intrusion detection system, examines different detection approaches including the one that our answer utilizes, and gives an essential structure to creating intrusion detection systems. [4] Gives a phenomenal investigation of the nature of intrusions and detection techniques.

A considerable literature, including a paper by [5], additionally exists that talks about the assessment of techniques utilized for intrusion detection, including the statistics-based anomaly detection examined in this paper.

Enterprises spend a lot of their computer security spending plan on keeping attacks from outside programmers who are either endeavoring unauthorized access or presenting harmful code, for example, worms and infections into the enterprises. Insider attacks are more difficult to distinguish and obstruct than outsider attacks since they happen inside the venture firewall by users who give off an impression of being trusted in the wake of going through standard confirmation and authorization forms. Building up a resistance against insider attack must strike a harmony between simplifying access to help user efficiency and actualizing a sensible level of security. Legitimate and moral protection issues exist when an insider attack arrangement is actualized, despite the fact that those issues are outside the extent of this paper. One approach to limit the effect on users is to play out a post-investigation of the log records made by security screen applications, middleware programs, application servers, and other endeavor applications. This procedure distinguishes the insider attacks after the data has been accessed instead of as they are happening.

An examination [6] demonstrated that 33 percent of data security attacks started from internal employees, while 28 percent originated from ex-employees and company partners. An overview [7] found that 22 percent of the reacting associations had encountered basic system interruption to their association because of an insider attack, with seven percent reacting that the occurrences had brought about loss of customers.

In this paper, we talk about the sort of insider attack in which employees of a venture engage in an example of resource-access conduct that surpasses what is vital for their business duties. That is, while employees may have general authorization for accessing particular applications and data over the span of playing out their jobs, they access extreme amounts of data or data that is irrelevant to their allocated undertakings. [7] Found that authorized users with legitimate records did 78 percent of insider attacks, and in 43 percent of the cases, the people utilized their own particular user ids and passwords while accessing the data.

In spite of the fact that we are concentrating on representative conduct, the techniques we depict apply to business partners of a venture who approach rights to delicate applications and data.

Example of insider misuse detailed as of late incorporate the accompanying:

- A account manager changed the address of a record he oversaw, had another credit card and PIN sent to his own address, and after that utilized the card to pull back cash from the credit card account.
- A company selling individual data to different organizations and government offices had a lot of data accessed in an unauthorized way by users who had set up counterfeit organizations with a specific end goal to give off an impression of being real customers.
- A previous help work area representative at a correspondences company conceded to a plan to take and offer 30,000 consumer credit reports of customers of that company.

II. RISK MINIMIZATION STRATEGIES

After risks have been identified and assessed, organizations can choose between different risks minimization strategies.

- *Avoiding*

Results in eliminating the vulnerabilities or the assets exposure to the threat. This strategy is applied in cases when the severity of the impact of the risk outweighs the benefit that is gained from having or using the information.

- *Reducing*

The assets exposure to the risk by implementing appropriate technologies and tools (such as firewall, antivirus systems, etc.) or adopting appropriate security policies (i.e. passwords, access control, port blocking). Reduction or ‘ mitigation’ is the primary risk management strategy.

- *Transferring*

The risk responsibility by partially shifting the risk to either outsourcing security service provision bodies or buying insurance.

- *Accepting*

The security measures as a cost of doing business. Risk retention is a reasonable strategy for risks where the cost of investment or insuring against the risk would be greater over time than the total losses sustained.

III. LITERATURE SURVEY

A. This research work is based on detecting insider attack or adversity that can be classified as anomaly. The process is detection is based on statistical methods. To demonstrate its working they have conducted experiments with two scenarios and found their method better in detection as compared to previous methods of anomaly detection. Their work also has response and alert system.

B. In this research work the authors have used the concept of ‘ decoy’ to evade adversity attacks. The work is basically done on the distributed computer platform. The authors have claimed in their research work, that their method gives extra-ordinary level of security in cloud due to fact, their experimental results revealed high level of accuracy. The concept of decoy is to show the attacker a fake resource like server, on which the attackers waste his energy and resources.

C. These authors have inferred from the current situation of network and security status that the ‘ insider’ attack detection is one of the most challenging tasks. Therefore, to overcome this issue, the author have designed an algorithm that works based on multiple files of the organizational structure or in simple words means that, it works at all level of organizational security. This attack is avoided by doing sampling and implementing a method that distinguished between genuine attacks actual attacks.

D. These authors have used the concepts psychology to address the problem of insider attacks they had developed a methodology called structural anomaly detection. This method uses diagrams investigation element tracking, machine learning method to search the oddities in the cloud / network.

E. These researchers believe the use of decoy data, files documents can help us to solve the problem of insider attacks. Therefore, they have developed an algorithm that works on the concept of decoys. After implementation and testing their algorithm they have claimed to find low fake alarm rate application for detecting the insider attack.

F. This research work basically investigates three aspects of it security. The first issue these author talk is about the ‘ trust’ that is not maintained by the user of the computing service the second issue they are discussing is tradeoff between the security measures later and the value of insider attacks assets. The third though expressed of this research work is about the magnitude of the insider attack problems. The work on research for insider threat (WRIT) highlighted difficulties particular to the IT issue, assessed existing promising methodologies and investigated experimentation potential outcomes for assessment of solution methodologies.

G. This paper primarily focuses on the usage of FTP records information for detecting the adversity. By tracking what is getting upload & download. Then, the researcher also suggests tracking of sensitive information also.

H. In this research work, the authors are basically talking about the ‘ collaborative’ insider attacks. These collaborative insider attacks are harder to detect and understand due to dynamic nature of the attacks. The algorithm used here uses multiple calculations for distinguishing the inside attack from normal user to simulation results claimed here show that the algorithm is good in detecting collaborative attacks.

IV. METHODOLOGY

In this section we will present the proposed work in details. The architecture of proposed framework is shown in Fig 1.

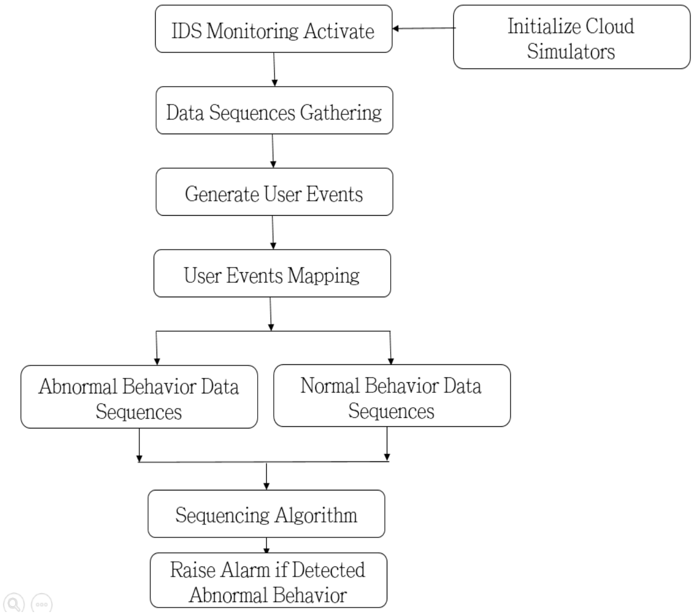

IDS Monitoring Activate
Initialize Cloud Simulators
Data Sequences Gathering
Generate User Events
User Events Mapping
Abnormal Behavior Data Sequences
Normal Behavior Data Sequences
Sequencing Algorithm
Raise Alarm if Detected Abnormal Behavior

Fig 1:- Proposed System Architecture

A. Phase I

This steps incorporates the working of the cloud simulation, for this we have utilized discrete event model of reproduction.

- *Making of Data Center*

A server farm is the operational focus having physical machines. These machines have Virtual machines and the various facilities to process work given by the cloud broker.

- *Cloud User/Broker Entity*

It is element which amasses work for the data center(s). It might be a piece of gathering PCs which are sending work to the server farm.

- *VM Allocation and Migration Policies Units:*

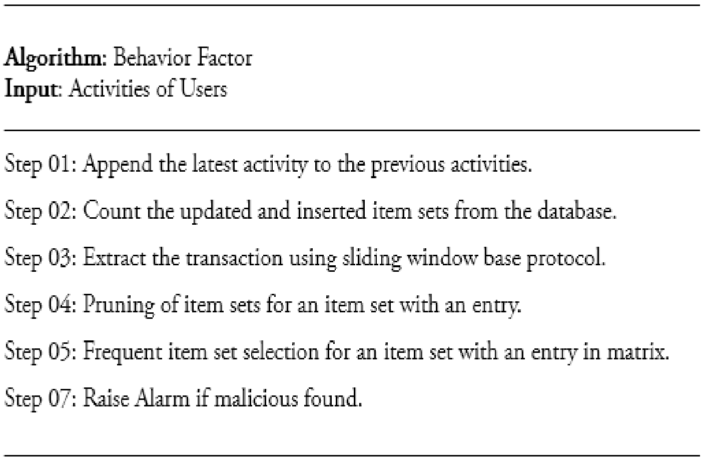
This term essentially implies how the function from the representative is appropriated to virtual machines of the server farm.

B. Phase II

Accumulation and Aggregation of Sequences: The different activities of users of companies are maintained by the databases and are regularly updated. The activities are encoded in numerical encodes and positioned by the succession mining calculation, which filter the database for most rare activity i.e. unusual utilizing Behavior Factors rules, which is fundamentally figured in view of sliding window time arrangement and conceivable response time measurements.

C. Behavior Factor based Sequence Data Analysis

Behavior factor are calculated for the dataset, which are helpful in determining the intrusion detection.

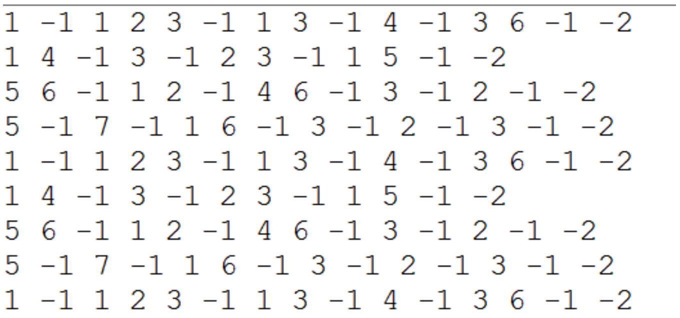


Algorithm: Behavior Factor
Input: Activities of Users

```
Step 01: Append the latest activity to the previous activities.
Step 02: Count the updated and inserted item sets from the database.
Step 03: Extract the transaction using sliding window base protocol.
Step 04: Pruning of item sets for an item set with an entry.
Step 05: Frequent item set selection for an item set with an entry in matrix.
Step 07: Raise Alarm if malicious found.
```

V. RESULT

The malicious behavior of the users are traced via the activities performed by the users. The user activity are continuously stored over the databases, which are required at the time of detection. The input dataset is shown in Fig. 2.



```
1 -1 1 2 3 -1 1 3 -1 4 -1 3 6 -1 -2
1 4 -1 3 -1 2 3 -1 1 5 -1 -2
5 6 -1 1 2 -1 4 6 -1 3 -1 2 -1 -2
5 -1 7 -1 1 6 -1 3 -1 2 -1 3 -1 -2
1 -1 1 2 3 -1 1 3 -1 4 -1 3 6 -1 -2
1 4 -1 3 -1 2 3 -1 1 5 -1 -2
5 6 -1 1 2 -1 4 6 -1 3 -1 2 -1 -2
5 -1 7 -1 1 6 -1 3 -1 2 -1 3 -1 -2
1 -1 1 2 3 -1 1 3 -1 4 -1 3 6 -1 -2
```

Fig 2:- Shows the input dataset which contains activity patterns of different users

Table 1. Shows the outcome of the proposed framework. The output obtained by analyzing the above dataset. It contains various number of instances. Normal and abnormal activity pattern found.

SNO	Attribute	Value
1	Number of Instances	Approx... 5000
2	Average number of abnormal activities sequences	63
3	Average number of normal activities sequences	4937

Table 1:- Results Summary

VI. CONCLUSION

In this experimental work we have possessed the capacity to discover an identification system that can do pattern discovery on the fly in view of the sequencing investigation of the hint of the activities of a cloud client, the proposed calculation is work effectively in giving quick reaction time as it is obvious from running arrangement of analyses and reproductions.

REFERENCES

[1] Nasr, P.M.; Varjani, A.Y., "Alarm based anomaly detection of insider attacks in SCADA system," Smart Grid Conference (SGC), 2014 , vol., no., pp.1,6, 9-10 Dec. 2014.

[2] S. J. Stolfo, M. B. Salem and A. D. Keromytis, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud," 2012 IEEE Symposium on Security and Privacy Workshops, San Francisco, CA, 2012, pp. 125-128.

[3] F. Kammüller and C. W. Probst, "Invalidating Policies using Structural Information," 2013 IEEE Security and Privacy Workshops, San Francisco, CA, 2013, pp. 76-81.

[4] O. Brdiczka et al., "Proactive Insider Threat Detection through Graph Learning and Psychological Context," 2012 IEEE Symposium on Security and Privacy Workshops, San Francisco, CA, 2012, pp. 142-149.

[5] J. Voris, N. Boggs and S. J. Stolfo, "Lost in Translation: Improving Decoy Documents via Automated Translation," 2012 IEEE Symposium on Security and Privacy Workshops, San Francisco, CA, 2012, pp. 129-133.

[6] Cybenko, G.; Moore, K., "Preface - WRIT 2012," Security and Privacy Workshops (SPW), 2012 IEEE Symposium on, vol., no., pp.xvii,xvii, 24-25 May 2012.

[7] Suresh, N.R.; Malhotra, N.; Kumar, R.; Thanudas, B., "An integrated data exfiltration monitoring tool for a large organization with highly confidential data source," Computer Science and Electronic Engineering Conference (CEEC), 2012 4th, vol., no., pp.149,153, 12-13 Sept. 2012.

[8] R. Pagliari, A. Ghosh, Y. M. Gottlieb, R. Chadha, A. Vashist and G. Hadynski, "Insider attack detection using weak indicators over network flow data," MILCOM 2015 - 2015 IEEE Military Communications Conference, Tampa, FL, 2015, pp. 1-6.

[9] Viet, K.; Panda, B.; Yi Hu, "Detecting collaborative insider attacks in information systems," Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on , vol., no., pp.502,507, 14- 17 Oct. 2012.

[10] D. Yachin,‘ Combating Insider Threats: The ApplicationLevel User Behavior Tracking Approach, IDC White Paper sponsored by Intellinx, 20.