Automatic Insider Threat Detection in E-mail System Using N-gram Technique

Aishwarya Potu[1], Snehal Mane[2], Akshay Kondhalkar[3], Pooja Talathi[4], Aparna Hambarde[5]

[1,2,3,4]BE Student, Dept. of Computer Engineering, KJCOEMR, Pune, India
[5]Prof, Dept. of Computer Engineering, KJCOEMR, Pune, India

Abstract - *Managing organisational cyber security is the threat that comes from those who operate within the organisation is one of the greatest challenges .It is becoming a serious and increasing concern and those who have fallen victim to such attacks suffering significant damages including reputation and financial. Hence an effective approach for insider threat detection is necessary. To classify documents in order to detect and prevent leakage of sensitive data n-gram frequency is used. In the system for detection of sensitive data using N-gram technique if the user sending sensitive information through email to outside network, it will get verified first on server-side using SHA, N-GRAM and Threshold based system. And after verification if threat found, the user gets blocked.*

Key Words: **Cyber security, Data leakage, *Insider* threat, N-gram, SHA, Threshold frequency**.

1. INTRODUCTION

The insider threat problem is one that is constantly growing in magnitude, resulting in significant damage to businesses and organizations alike. The employees who work in an organization are often trusted with highly confidential information such as intellectual property, financial records, and customer accounts, in order to perform their job. If an individual should choose to abuse this trust and act maliciously toward the organization, then their position within the organization, their knowledge of the organizational systems, and their ability to access such materials means that they can pose a serious threat to the operation of the business. Media has reported and exposed numerous cases in recent years of both government and businesses who have been compromised, where confidential information has been exfiltrated and exposed. The threat posed by insiders is real, and it requires serious attention by both organizations and individuals. Capelli *et al.* from the Carnegie Mellon University Computer Emergency Response Team (CMU-CERT) group identified three main groups of insider threat : information technology sabotage, theft of intellectual property, and fraud data. Over the years, technological advancements have meant that the way organizations conduct business is constantly evolving. It has become a common practice nowadays for employees to have access to large repositories of organization documents electronically stored on distributed file servers. Many organizations provide their employees with company laptops for working while on the move and use e-mail to organize and schedule appointments. For hosting meetings across the globe, services such as video conferencing are frequently used . Employees are constantly connected to the Internet where they can obtain information of anything that they require for conducting their workload. The technological advancements could potentially make it easier for insiders to attack. One advantage of the organizational view to this is the capability of capturing activity logs that may provide insight into the actions of employees. Due to the sheer volume of activity being conducted by employees every day, analyzing such activity logs would be infeasible for any analyst. What is required is a capability to analyze individual users who conduct business on organizational systems, to assess when users are behaving normally and when users are posing a threat.

2. LITERATURE SURVEY

1) Title- Automated Insider Threat Detection System Using User and Role- Based Profiling Assessment :

In this paper, systematic approach for insider threat detection and analysis based on the concept of anomaly detection is presented. The system constructs a tree-structured profiles with reference to given a large collection of activity log data that describe individual user activity and combined role activity. They have constructed a feature set representation that describes the observations made for each day and the variations that are exhibited between the current day and the previously observed days[1].

2) Title- Caught in the Act of an Insider Attack :

In this paper, a systematic approach for insider threat detection and analysis is presented. The system constructs a tree-structured profile from activity log data that is collected on users within the organizations for each user and for each role. This allows multiple activity types to be represented in a unified approach, that helps to support comparison between different users and associated roles[2].

3) Title- Word N-gram Based Classification for Data Leakage Prevention :

The objective of this paper is to prove the effectiveness of N-grams to measure the similarity between regular documents and existing classified documents. N-grams for data classification purposes is useable based on using the N-grams frequency to classify documents in order to detect and prevent leakage of sensitive data[3].

4) Title- Automated Big Text Security Classification :

In this paper, they have analyzed a dataset that contains actual formerly sensitive information annotated at paragraph granularity. Automated Classification Enabled by Security Similarity (ACESS) penetrates the complexity of big text security classification. Approach in this paper addresses the issue by partitioning a large text into smaller groups of similar paragraphs wherein multiple similarity-based classification models to predict a paragraph's security label[4].

5) Title- Visualizing the Insider Threat: Challenges and tools for Identifying malicious user activity :

In this paper, a visual analytics approach is proposed to detect the insider threat. With the help of a detailed activity visualization, it is possible to the analyst to explore the raw activity data and to check whether the user poses a threat to the organisation or not. The topics such as insider threat research, anomaly detection, and security data visualization are used. It helps to understand the detection and visualization which can help with the separation between the malicious and non-malicious activity[5].

6) Title- Mining Software Component Interactions to Detect Security Threats at the Architectural Level :

The main objective of this paper is to present an innovative data mining approach to detect anomalous behavior to interact among the software components at the architectural level. The EDS (Emergency Deployment System) is a real world software system which is used to define and evaluate the research. To detect more sophisticated threats it is important to monitor and assess the overall security posture of a software system at the architectural level. A use case driven mining framework is proposed with an adaptive detection algorithm to identify the potential malicious threats[6].

7) Title- A Model-Based Approach to Predicting the Performance of Insider Threat Detection Systems :

In this paper, a Model Based Approach is presented to predict the confusion matrix between insider threat detection system alerts and the truth whether the user is an insider or not. To evaluate a predictive model, datasets into which insiders have been injected or estimated the actual performance of the insider threat detection system are developed. A simple approach for modeling insider threat detection systems that relies on a small amount of the non user-specific data is described[7].

8) Title- Cyber security for Product Lifecycle Management A Research Roadmap :

In this paper, they have discussed present landscape with respect to the major cyber security risks. They have introduced a research focusing on cyber security in the context of product lifecycle management. It include research directions on critical protection techniques, including protection techniques from insider threat, access control systems and secure supply chains. An overview of DBSAFE, a system for protecting data from insider threat is presented[8].

9) Title- Dynamic Defense Strategy against Advanced Persistent Threat with Insiders :

In this paper, they have investigated the joint threats from the *APT attacker* and *insiders* over a long time-span within a general framework. The results in this paper can shade insights on practical system design for higher security levels facing the joint APT and insider threats[9].

10) Title- Modeling Insider Threat Types in Cyber Organizations :

In this paper, they have presented a computational framework to model insiders using relevant cultural, social, emotional, and other behavioral factors, along with technological factors, with the goal of categorizing them based on the type of threat they are likely to present to the organization. The proposed method provides an efficient relative measure of each person's awareness for different types of manipulations and it captures both short term and long term factors impacting their awareness[10].

3. TECHNIQUES

3.1 N-gram Technique

The N-Gram technique is used to break each word in the document into smaller character N-grams. To create an N-gram profile, the smaller character n-grams are rearranged based on the N-gram frequency. The created N-gram profile are compared with existing category N-gram profiles. The document are classified under the category with the smallest distance measure.

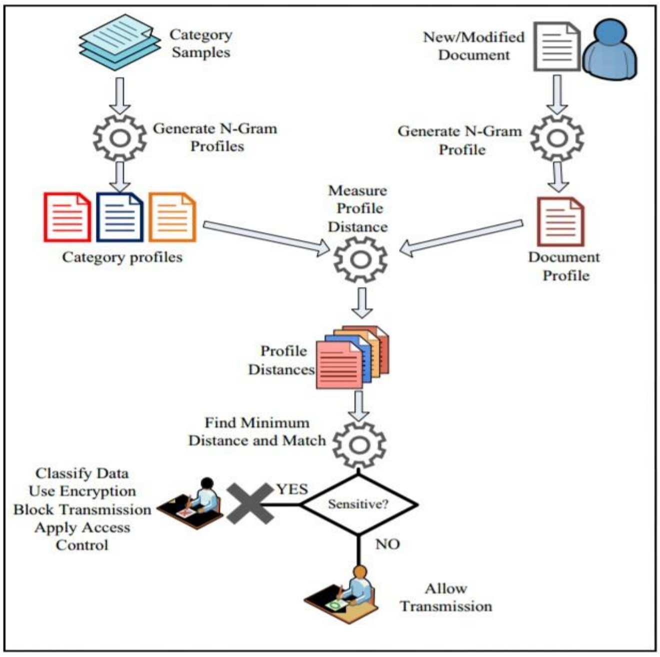

Fig-1: Word N-gram classification process

3.2 SHA

Secure Hash Algorithm 1 (SHA1) is a cryptographic hash function which is designed by the United States National Security Agency . SHA-1 produces a 20-byte hash value known as a message digest. A SHA-1 hash value is a hexadecimal number i.e 40 digits long. It execute by transforming the data using a hash function. It uses an algorithm that consists of modular additions, bitwise operations and compression functions. A fixed size string produced by hash function looks nothing like the original. To be one-way functions the algorithms are designed i.e. once they are transformed into their respective hash values then it is virtually impossible to transform them back into the original data. SHA algorithms are designed and modified with increasingly stronger encryption technique in response to hacker attacks.

3.3 Threshold Frequency

Threshold is a value. We associate the Threshold to a statistic. Data is collected for that statistic, then it is compared with the associated Threshold value. If the collected data value does not warrant the Threshold value, then it indicates that this type of data might lead to poor performance of the network or device. Threshold value is set up along with a level such as the maximum value, equal value and the minimum value. When the collected value exceeds the threshold value, notification, which we receive is in the form of a Threshold Event. An event is an occurrence of any action. Whenever a threshold value has exceeded, a threshold event is generated. Also, every Threshold event is associated with a Severity to denote how critical the situation is. The total count number of sensitive word frequency is compared with threshold value, the log is maintained and the appropriate action is taken, i.e. in email system, to block the mail or send it.

4 EXISTING SYSTEM

A tree-structure profiling approach incorporates the details of activities done by each of the user and job role and then use this to obtain a consistent representation of features that gives a rich description of the user's behavior. Deviation can be assessed with reference to the amount of variance that each user exhibits across multiple attribute by comparing against their peers[1].

Following are the requirements of the detection system :

1) The system must be featured in such a way that it should be able to determine a score for each of the user that relates to the threat that they currently pose.
2) The system should be expert to deal with various forms of insider threat, including sabotage, intellectual property theft, and fraud data.
3) The System should have the ability to deal with the unknown cases of insider threat, whereby the threat is decided to be an anomaly for that user and for that role.
4) The system also should be able to detect the threat that an individual poses based on how this behavior deviates from both their own previous behavior and the behavior exhibited by those in a similar job role.

5 PROPOSED SYSTEM

The main objective of the system is to detect the suspicious mail sent by the insider threat. The mail is being sent from client using SOAP (Simple Access Object Protocol). Once it is received on the server side, JAVA API is used to send email to particular receipt.

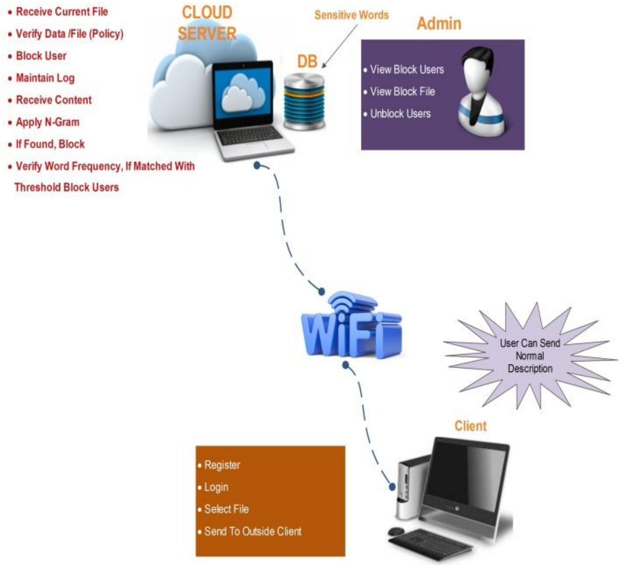

Fig-2: Proposed system scenario

Every authorized registered client will be given a login Id and Password to access to the system. On the server side database is maintained. The database contains all the sensitive word list, files and documents. Admin maintains the email logs, manage block list, manage white list and black list. The admin has the right to block the user if any illegal activities are caught

6. CONCLUSION

With the reference to the previous work done, the objective of the project is to develop an application to detect insider threat in E-mail system. In this system when the user sending sensitive information to outside networks, it will get verified first on server-side using SHA, N- GRAM and Threshold based system. The log is maintained by Admin. And after verification if sensitive information found, the user gets blocked.

REFERENCES

[1] "Automated Insider Threat Detection System Using User and Role- Based Profiling Assessment", Philip A. Leg, Oliver Buckley, Michael Goldsmith, and Sadie Creese, 2015

[2] "Caught in the Act of an Insider Attack: Detection and Assessment of Insider Threat ", Philip A. Legg, Oliver Buckley, Michael, Goldsmith and Sadie Creese ,Cyber Security Centre, University of Oxford, UK. , 2015

[3] "Word N-gram Based Classification for Data Leakage Prevention", Sultan Alneyadi, Elankayer Sithirasenan, Vallipuram Muthukkumarasamy, Faculty of Science, Environment, Engineering and Technology, Griffith University Gold Coast Campus, Australia, 2013

[4] "Automated Big Text Security Classification", Khudran Alzhrani, Ethan M. Rudd, Terrance E. Boultand C. Edward Chow, University of Colorado at Colorado Springs Department of Computer Science Vision and Security Technology (VAST) Lab, 2015

[5] "Visualizing the Insider Threat: Challenges and tools for Identifying malicious user activity", Philip A. Legg, 2015

[6] "Mining Software Component Interactions to Detect Security Threats at the Architectural Level" , Eric Yuan And Sam Malek, 2016.

[7] "A Model-Based Approach to Predicting the Performance of Insider Threat Detection Systems", Shannon C. Roberts, John T.Holodnak, Trang Nguyen, Sophia Yuditskaya, Maja Milosavljevic, William W. Australian MIT Lincoln Laboratory, 2016

[8] "Cyber security for Product Lifecycle Management A Research Roadmap", 2015.

[9] "Dynamic Defense Strategy against Advanced Persistent Threat with Insiders", Pengfei Hu, Hongxing Li Hao Fu, Derya Cansever and Prasant Mohapatra, Department of Computer Science, University of California, Davis, USA

[10] "Modeling Insider Threat Types in Cyber Organizations", Eunice E. Santosa,c, Eugene Santos Jr. b,d, John Korah a,e, Jeremy E. Thompson b, Vairavan Murugappana, Suresh Subramaniana, Yan Zhao B, 2017

[11] P. A. Legg et al., "Towards a conceptual model and reasoning structure for insider threat detection," J. Wireless Mobile Netw., Ubiquitous Comput., Dependable Appl., vol. 4, no. 4, pp. 20–37, Dec. 2013.

[12] J. R. C. Nurse et al., "Understanding insider threat: A framework for characterising attacks," in Proc. IEEE SPW, 2014

[13] L. Spitzner, "Honeypots: Catching the insider threat," in Proc. 19th IEEE ACSAC, Las Vegas, NV, USA, Dec. 2003

[14] G. B. Magklaras and S. M. Furnell, "Insider threat prediction tool: Evaluating the probability of IT misuse," Comput. Security, vol. 21, no. 1, pp. 62–73, 1st Quart. 2002.

[15] J. Myers, M. R. Grimaila, and R. F. Mills, "Towards insider threat detection using web server logs," in Proc. 5th Annu. CSIIRW—Cyber Security Inf. Intell. Challenges Strategies, New York, NY, USA, 2009

[16] O. Brdiczka et al., "Proactive insider threat detection through graph learning and psychological context," in Proc. IEEE Symp. SPW, San Francisco, CA, USA, May 2012

[17] W. Eberle, J. Graves, and L. Holder, "Insider threat detection using a graph-based approach," J. Appl. Security Res., vol. 6, no. 1, pp. 32–81, Dec. 2010.

[18] "AD2: Anomaly Detection on Active Directory Log Data for Insider Threat Monitoring", 2016