Paper ID:CSEIT12

INSIDER DATA THEFT PREVENTION USING BEHAVIOR PROFILING

Ms.Mayuri M.Bhosale
M. E. Student, Department of Computer Science & Engineering, D. Y. Patil College of Engineering & Technology, Kolhapur
Mr. G. A. Patil
HOD, Department of Computer Science & Engineering, D. Y. Patil College of Engineering & Technology, Kolhapur

Abstract –In the commercial organizations especially small and medium scale businesses a lot depends on outsourcing of data which comes with more risk for insider data theft attacks. Insider data theft detection is an emerging field developed with opportunities for new research methodologies. Insider data theft attacks are caused by masquerader stealing a valid user's identification and using it to mimic the authenticate user.

We present a novel anomaly detection approach where behavior profiling will be done by combining different classifier to build a sustainable ecosystem that can mitigate frauds efficiently. The system creates standard user behavior model by extracting features of user activity. Current user behavior is compared with the standard user behavior model of that user. If difference is observed then it will be considered as possibility of malicious activity. Ensemble of classifier is produced using Naïve Bayes Classifier and One-class support vector machine (SVM). The implemented system prevents unauthorized and illegitimate access to the system and provides security to the user's data by profiling user's behavior.

Keywords-- Insider data theft, Behavior profiling, Naïve Bayes Classifier, One Class Support Vector machines

I.INTRODUCTION

There is not very great awareness about fraud and misconduct among corporate of India. This is considered as one of the top threats to cloud computing by the Cloud Security Alliance. Insiders may get the credentials of authorized user by hacking password for accessing system dishonestly. The insider data theft can be considered extremely hazardous because of direct access to sensitive data on the system.

The Twitter incident is one of the well known examples of an insider data theft attack . Customer's accounts of twitter including the account of U.S. President Barack Obama, were unauthorizedly accessed and their documents are illegally ex-filtrated to website TechCrunch.

Much research in security is focusing on solutions of preventing malicious insider data theft. Lots of mechanisms are proposed to secure users data by encryption and typical access control mechanisms. However it is observed that these methods have failed to protect damage perpreted by malicious insider activity. To overcome this limitation, proposed system presents a strong detection mechanism where profiling user search behavior will be created by combining more than one classifier to reduce false positive rate.

The proposed approach could improve accuracy over prior mechanisms and will help to provide the superior and intelligent level of security in terms of insider attacks.

II.LITERATURE SURVEY

Stolfo et al proposed a combined approach for detecting masquerade attacks [1]. The authors focused on modeling user search behavior with a baiting technique to reveal an attacker's malicious intent. They hypothesized and showed that a masquerader would engage in search activities different from those of the legitimate user in terms of their volume and frequency.

Maloof et al applied a user behavior profiling technique to detect malicious insider activities which violated `Need-to-Know' policy [2]. In order to identify bad insider behavior, they defined the malicious user scenarios and had to combine results different sensors through a Bayesian net. Although the few attack scenarios tested were detected, there was no real evaluation of the false positive rate associated with the overall classifier.

Hershkop et al surveyed that most of the prior user behavior profiling work focused on auditing and modeling sequences of user commands including work on enriching command sequences with information about command arguments. A thorough review of these machine learning techniques can be found in this survey [3]. The detection rates of these anomaly detection techniques ranged between 75.8% and 26.8%, with false positive rates ranging between 1% and 7%. These results are obviously far from satisfactory.

Chawla et al presented a novel approach to distributed learning using fuzzy clustering [4]. This intelligent method of partitioning a dataset is compared to simpler, random methods of partitioning. The results presented in this paper suggest that for very large datasets, the creation of ensembles of classifiers can perform reasonably well.

Dzeroski et al empirically evaluated several state-of-the art methods for constructing ensembles of heterogeneous classifiers with stacking and shown that they perform comparably to selecting the best classifier from the ensemble by cross validation [5]. They had proposed a new method for stacking which uses multi-response model tree at the meta-level.

McCallurn et al used two common models used in Naïve Bayes Classifier, one is the multi-variant Bernoulli model, and the other is the multinomial model [11]. In the multivariate Bernoulli event model, a vector of binary

attributes is used to represent a document, indicating whether the command occurs or doesn't occur in the document. The multinomial model uses the number of command occurrences to represent a document, which is called "bag-of-words" approach, capturing the word frequency information in documents. According to McCallurn's result, multi-variants Bernoulli model performs better for small vocabulary size, and the multinomial model usually performs better at larger vocabulary size.

Scholkopf et al proposed a method to adapt the SVM algorithm [13] for one-class SVM, which only use examples from one-class, instead of multiple classes, for training. The one-class SVM algorithm first maps input data into a high dimensional feature space via a kernel function and treats the origin as the only example from other classes. It then iteratively finds the maximal margin hyper plane that best separates the training data from the origin.

Existing algorithms used for modeling user behavior makes use of statistical features, such as the sequence of user commands or co-occurrence of multiple events combined through logical operators. The anomaly detectors built using these algorithms suffer from low accuracy and from high false positive rates. One way to overcome this limitation is to combine some base classifiers to create one ensemble of classifiers. So proposed system offers a good solution against this limitation where each classifier uses a different modeling algorithm to profile user behavior.

III.PROPOSED SYSTEM

Following Figure shows the Architecture of the insider data theft prevention system:

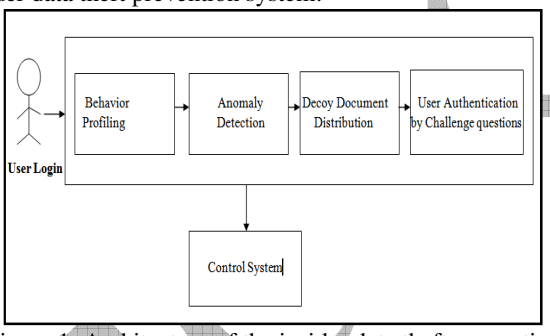

Figure 1: Architecture of the insider data theft prevention system

In the above system behavior profiling detects abnormal user behavior which is the base of system. Then it monitors for abnormal behaviors that show large deviations from the derived base. The system prepares a normal user model Nu that models the user's behavior by fetching distinguishing features and measures the difference between actual user behavior and the past user behavior as defined by the normal user model Nu. The distance Di is compared in order to determine whether there is enough proof for masquerade activity or not.

Insider data theft prevention system is implemented using following modules:

a) Validating user logins

The application is deploy on a system, which will be used to validate system. User logins are the imperative inputs for system which will consist of the following options:

1. It will store necessary user details and provides at least three challenge questions at the time of account registration.
2. It will allow strict entry time checking system, where the user randomly selects challenge questions on each login.

User will choose the challenge question at the time of account registration.

b) User access behavior profiling

While monitoring behavior of user, abnormal behavior can differ from normal user behavior. Standard user model will be prepared by extracting distinguishing features such as speed of pressing keystrokes, mouse movements etc. The present work focuses to reduce feature set by selecting minimum distinguishing features among them.

Also ensemble of classifier is created for reducing low accuracy of anomaly detection. Some of the following classifiers are combined in the present work.

i) One-class support vector machine

The one-class SVM algorithm first maps input data into a high dimensional feature space via a kernel function and treats the origin as the only example from other classes. Considering that training data set $x_1, x_2, x_3, \ldots x_n \epsilon$ F,n is the feature mapping X ->F to a high-dimensional space, we can define the kernel function as:

$$k(x, y) = (F(x) \times F(y))$$

ii) Naïve Bayes Classifier

The multinomial model is frequent model of Naïve Bayes classifier. Using the standard bag-of-words approach, each command block is represented by a feature vector

where n_i (d) is the number of times command c_i appears in the command block d Similarly, given $p(c_i \mid u)$, which is the frequency count computed for command c_i for user u in the training data.

c) Anomaly detection

The system is developed where current user behavior is modeled. It is compared with the standard behavior model of that user. If the difference is exceeding the limit, then that user is suspected to be masquerader. It will be the first suspecting alert of the detection system. User will be exposed to next module only if this alert is generated. If the current user behavior is same as the past behavior, there is no need to traverse the next modules and the user is allowed to continue his work on original data.

IV.IMPLEMENTATION DETAILS

a) Validating user logins

This module is used to validate the insider data theft attack detection system. So logins for administrator and user are implemented in this module. It stores 3 secrete questions at the time of account creation along with the other registration details such as name, password, email, address etc. Choice of selecting one question among the group of three questions will be done by user at the time of account creation. Also it will ask to enter time span for which user is going to use the system. Time span entered by user will be used for session management. The speed of pressing the keystrokes is extracted as a feature and this is used to distinguish the suspicious and normal user activity. The ip address on which user is working is also extracted as a classifying feature.

b) User access behavior profiling

Ensemble of classifier is created for reducing low accuracy of anomaly detection System. One class SVM and Naïve bayes classifiers are combined in this work.

Anomalous user behavior can vary from normal user behavior. According to this assumption standard user model is prepared by extracting distinct features by using one class SVM. All features mentioned below are the key parameters to check whether the user behavior is normal or suspicious. If any of the features show variation from normal behavior, it is treated as indication of masquerade attack.

1. Attempts towards user login.
2. Timing of login.
3. The ip address of system from which user logs in.
4. Speed of pressing keystrokes by logged user.
5. Habit of using mouse or keystrokes for submitting.
6. Attempts towards challenge questions.

All features mentioned above are the key parameters to check whether the user behavior is normal or suspicious. If any of the features shows variation from normal behavior, it is treated as indication of masquerade attack.

A set of challenge questions is asked to the user at the time of registration. Answers are stored using bag-of-words approach of multinomial model of naïve bayes classifier, creating vocabulary of each user. To improve accuracy of overall detection system random questions are asked rather than asking same question. The multinomial model checks whether entered answer is present or not in real users vocabulary. Incorrect answer to the first randomly asked question will lead you to the next question. Count of failed attempts towards the question is considered as the indicative for suspicious activity.

c) Anomaly detection

The system is implemented such that current user behavior will be compared with the standard behavior of that user. If the difference is exceeding the limit, then that user is suspected to be masquerader.

Features mentioned in previous modules are monitored. If any of the currently extracted features behaves differently than the past behavior, alert is generated. Whenever alert by anomaly detection is generated, decoy information is supplied immediately.

'Normal' alert is generated if user behavior is same as standard behavior of that user. 'Attacker' alert is generated if user has downloaded the decoy document. 'Suspicious'alert is generated if following circumstances arise.

- If user logged in from diffrent ip address.
- If user frequently enters the incorrect password.
- If speed of pressing keystrokes of user mismatches.
- If user gives frequently incorrect answers to security questions.
- If user tries to log in rather than usual timing.

V. RESULTS

The control system represents an interface to view the malicious insider accesses. It allows the administrators to implement grant/discard policies for the users. Administrator blocks the masquerader by denying access to the systems original data. The administrator follows following policies to generate alert on the basis of behavior profiling:

- If one or two of the deciding features behaves abnormally then suspicious alert is generated and that user is subjected towards security questions.
- If more than two of the deciding features behave abnormally then attacker alert is generated and that user is supplied by decoy document.
- If all of the above features deciding abnormally then normal user alert is generated and that user is supplied by original document.

Figure 2 show different alerts generated on admin account. 'Normal' alert is generated if user behavior is same as standard behavior of that user. 'Attacker' alert is generated if user is proved as masquerader. 'Suspicious' alert is generated if user activity seems to be suspicious.

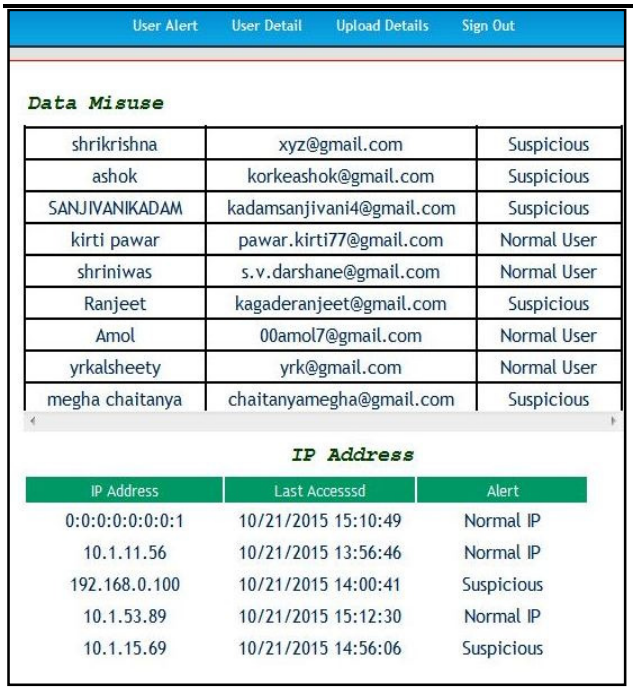

Figure 2: Alerts generated on Admin account

System maintains logs of user activity as shown in Figure 3.Start time and end time as well as status of that user whether he is active or inactive is recorded.

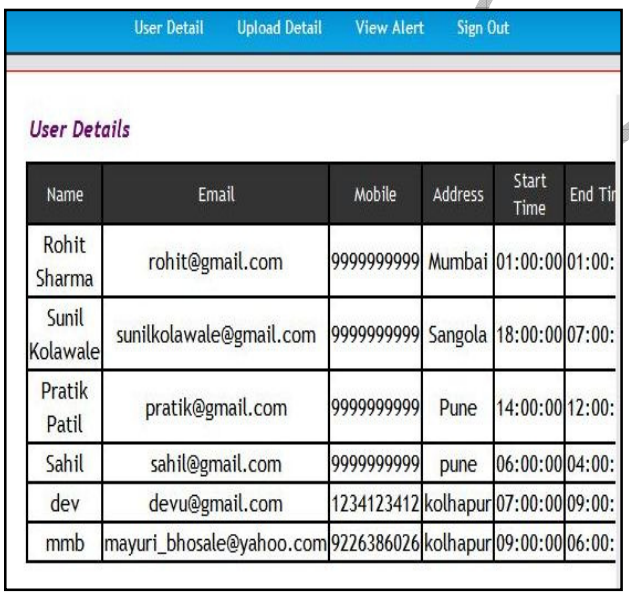

Figure 3: Logs maintained on admin account

System maintains upload details as shown in Figure 4.details of file uploaded such file name, size, date of uploading is stored for maintaining log records.

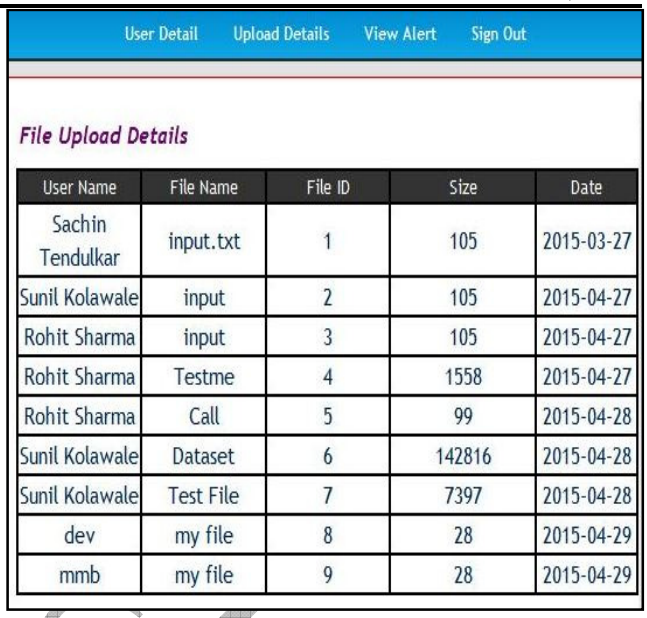

Figure 4: Upload details on Admin account

VI. CONCLUSION AND FUTURE SCOPE

In insider data theft prevention system we present the approach with ensemble of classifiers. Insider attack is very difficult to identify so the proposed system helps to provide the higher and intelligent level of security in terms of insider attacks. The approaches are based on the predefined user behaviours and monitoring.System is implemented in such a way that it could provide an integrated detection approach where profiling user search behavior is combined with two classifiers in order to prevent malicious insider data theft attacks. As part of future work, system will be modified in such way that behavior profiling is combined with the baiting approach using decoy documents to make the system more secure.

REFERENCES

[1] Salvatore J. Stolfo,Malek Ben Salem, Angelos D. Keromytis,“ Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud”, IEEE Symposium on Security and Privacy Workshops,July 2012.

[2] Maloof M.A.and Stephens et al,“ Detecting Insider Data Theft of Trade Secrets” ,published by the ieee computer and reliability societies ,november/december 2009 .

[3] Shlomo Hershkop et al “A survey of insider attack detection research”, In Insider Attack and Cyber Security: Beyond the Hacker, Springer(2008).

[4] Chawla, N. V., Eschrich S. and Hall L. O., “ Creating ensembles of classifiers.” In Proceedings of the 2001 IEEE International Conference on Data Mining (Washington, DC, USA, 2001),IEEE Computer Society, pp. 580-581.

[5] Dzeroski S., and Zenko B. "Is combining classifiers better than selecting the best one" In Proceedings of the Nineteenth International Conference on Machine Learning (San Francisco, CA, USA, 2002), ICML '02, Morgan Kaufmann Publishers Inc, pp. 123-130.

[6] Ben-Salem, M., and Stolfo, S. J., " Detecting masqueraders: A comparison of one class bag-of-words user behavior modeling techniques." In MIST '10: Proceedings of the Second International Workshop on Managing Insider Security Threats, Japan (June 2010), pp. 3-13.

[7] M. Ben-Salem and S. J. Stolfo, "Combining a baiting and a user search profiling techniques for masquerade detection," In Columbia University Computer Science Department, Technical Report#cucs01811,2011.

[8] Lingaswami, G. Avinash Reddy, "Offensive Decoy Technology For Cloud Data Attacks.", International Journal of P2P Network Trends and Technology(IJPTT)–Vol.3 Issue 10-Nov 2013.

[9] Cloud Security Alliance, "Top Threat to Cloud Computing V1.0," March 2010. [Online]. Available:https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[10] M. Arrington, "In our inbox: Hundreds of confidential twitter documents," July 2009. [Online].Available: http://techcrunch.com/..

[11] A. McCallurn, K. Nigam, "A Comparison of Event Models for Naive Bayes Text Classification", AAAI-98 Workshop on Learning for Text Categorization, 1998.

[12] T. M. Mitchell, Bayesian Learning, Chapter 6 in Machine Learning, pp. 154-200. McGraw-Hill, 1997.

[13] B. Scholkopf, J.C. Platt, J. Shawe-Taylor, A.J. Smola, and R.C. Williamson, "Estimating the support of a highdimensional distribution". Technique report, Microsoft Research, MSR-TR-99-87, 1999