International Journal of Future Generation Communication and Networking
Vol. 13, No.2s, (2020), pp. 1566–1571

Literature Survey – Automated IDPS for Database Intrusion Attacks from Insiders

Mr. Akshay Kodolikar,
School of CET,
MIT WPU PUNE.

Prof. Dr. Balaji M. Patil
School of CET,
MIT WPU PUNE.

Abstract

Information repositories are facing huge number of cyber security threats, majority of which are intended by insiders. Insiders reside behind the enterprise-level security defense mechanisms and often have privileged access to the network resources, detecting and preventing insider threats is a complex and challenging problem. Current database management systems not enough for new high-tech attacks, so need of intelligent Database Intrusion Detection and Prevention System is required as additional security layer.

Keywords—*Insider,RDBMS, IDS, IDPS,RPA, ID3,Deep Learning,Machine learning.*

I. INTRODUCTION

Internal threats can be defined as computer security threats that occur in an organization. These threats can be from employees or salespeople or everyone who has a valid intranet access, including a former employee.

Insider attempts to filter out confidential data have become a serious threat to the enterprise. Common data security techniques, such as access control and encryption must be used along with enhanced techniques for detecting anomalies in accessing data that may indicate exfiltration attempts. The database attack is divided into two categories Internal Attack and External Attack. Insider Attacks are performed by legitimate users who try to abuse their rights, such as breaking privileges levels. The external attack is performed by a person who does not have rights to access the application or information repositories, though the access restrictions applied somehow insider's access and modify information. They also sell private information to the company's competitor or who pays enough for that information. *A*ttack is frequently followed by an attacker, major controlling terminal, and agency terminal and attack target. Intrusion detection can be either signature-based or anomaly-based. Signature based analysis use existing attack patterns and characteristics.

Each new transaction is analyzed if it corresponds to an existing attack pattern, and if it is successful, then these transactions marked as harmful. The signature-based method does not use mining techniques. Anomaly based approach maintains normal behavior vs. new behavior when new transaction behavior differ significantly then it is marked as threat or an anomaly. Anomaly-based intrusion detection system use clusters, association rules, etc. to represent normal behavior and anomaly. Anomaly based approach use mining for Intrusion Detection. Firewall is the first line of defense against the computer while Intrusion detection come immediate next it is mainly for monitoring and protecting your computer from unauthorized access.

II. BACKGROUND

Despite nearly 20 years of research, Monitoring and preventing internal threats with technological achievements, the efforts are greatly accelerated but none have achieved relief from insider threats. This can be because of one or more of the following: Reason:

1) Some options do not appeal to themselves for the signs of a bad insider, at the early stages.

2) Most decisions depend on the individual source information, management to mitigate information threats.

3) Traditional analytic methodologies are time consuming as knowledge extraction and features or rules extraction takes major amount of time.

III. LITERATURE SURVEY

In this section existing work is discussed. Researchers have used bot Supervised and Unsupervised learning practices for IDPS.

[1] Article authors Mehul S. Raval et al In the paper used machine learning techniques for anomaly detection. They also applied linear regression followed by Cook's and Mahalanobis distance to identify suspicious activities of the user. These activities are analyzed by SVM and Neural network for unusual behavior detection. They also stated use of behavioral analysis and sentiment analysis for future work to detect the intrusion more precisely.

[2] Article authors Kaushal Bhavsa et al in this paper include approaches using deep learning for emerging internal threats, based on historical and current behavioral analysis. They wanted to demonstrate a technology to detect a potential threat to the organization based on user activity. They also states that prior to the attack, attacker behavior becomes unusual. Which includes daily events such as login / logout, internet access, file access, etc. authors concludes by studying user behavior, you can visualize internal threats to your organization. Thanks to deep learning, the organization quickly identifies them by behavioral patterns which show future threats.

[3] Article authors Souparnika Jayaprakash et al in this paper presented complete database intrusion detection system Prevents intrusive internal and external attacks. The proposed system is a flexible enough that can be customized with increasing complexity and dynamics of the database attacks. Proposed architecture is based on anomaly detection mechanism implementing role-based access control (RBAC).Novel structure named octraplet is used for query storage. System uses supervised Naive Bayesian classifier machine learning method for detecting abnormal events. Proposed method can also improve detection rate.

[4] Raji Ramachandran et al Authors have used role based mechanisms for accessing databases, the identification system is recommended. Machine learning techniques are important which provides classification for access control breach in role-based control system this will help prevent internal attacks. The experimental results show that the system can identify intrusions with effective high level accuracy and high F1 rate.

[5]Preeti Mishra et al have proposed Intrusion detection is an important defense challenge in today's networked world. Quite a lot Machine-learning based technique has been developed but they are not very successful in their mythologies to identify all types of intruders. Details of this article analyze various machine learning methods. Authors have shared results of analyzed techniques in this particular article.

[6]Qussai Yaseen Et al in This article proposes a framework to predict and mitigate the threat of internal database systems. The proposed model provides architects and database administrators with a more robust method for predicting intent of user. Furthermore, it provides a way to monitor internal knowledge base that grows in business. Framework monitors real-time internal attacks that can be initiated. Furthermore, this article provides rescue strategies for eliminating problems based on the threatening principles found in the context. Finally proposed model was tested to demonstrate its feasibility and viability.

[7] Derui Ding et al in this article summarizes the recent progress in security control and industrial cyber-

attack detection from the perspective of control theory. Firstly, a typical system model is summarized to meet the requirements of performance analysis from an engineering standpoint, for Network attacks: such as denial of service, replay and fraud attacks. It discusses visibility, security and resilience, and stability. This can be useful for controlling industrial CPS attacks. Furthermore these are checked according to the detection method.

[8] Hagit Grushka-Cohen et al In this article, authors have proposed a new algorithm Cyber Rank which expertise effectively even though lowers no of samples provided. In the initial trainings system does better than other algorithms. Create comprehensive examples and annotate models Created and guided by Priority learning algorithm. Algorithm captures anomalies in database transactions and analyzes risks to your organization. Cyber Rank outperforms all other methods for cold start scenario with error reduction of 20%.

[9]Drashti Nandasana et al have stated database management system is insufficient to meet the new requirements High-tech attack, so a penetration detection system as additional layer of security is required. Over the last few years, many detection systems built using bugs or mining data dependencies and access methods. In this article, authors use the signature-based method, defines hierarchy of roles categorize users, and then make management easy. Their results seem committed to effective transaction transparency with higher accuracy and precision but needs human intervention for final outcome.

[10] Kalyan Veeramachaneni et al states the system has four keys Function: Big data behavior analysis platform, Anomaly detection method and security analyst feedback system and supervised learning module. These four Units move daily and compare it with the detection of the monitoring. Results show high average detection rate, false positives were reduced by five factors. Authors have validated data using actual dataset where there are billions of log lines. These result shows that system is capable of learning invisible intrusion patterns.

III. Proposed Architecture

The pioneers in machine learning-based IDS mainly focused on accuracy, efficiency and automatic feature extraction.
After detection of the intrusion at multiple instances the logs are analyzed by response team then after action is taken in earlier scenario.

Proposed system will not wait for response team or database administrator before taking action for database intrusion detection.

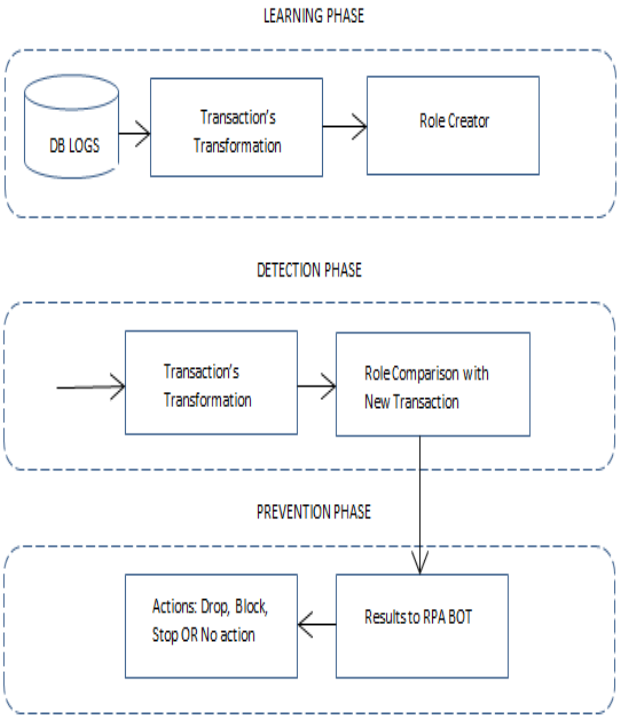

Fig1. Proposed Architecture

Proposed System is divided into three Phases

- Learning Phase
- Detection Phase
- Prevention Phase

Basic architecture learns the normal behavior vs. the unusual behavior for a particular user depending upon the database access logs. The role creator supports the learning phase to segregate the users into multiple roles, based on the access rights provided.

Detection phase as its name suggest does the work of detecting abnormal behavior. Machine learning algorithms help here to make accurate decisions based on its learning. After detecting the intrusions alarm as logs are created.

Once the logs are created the logs with higher risks are sorted from input file and provided to RPA BOT to take necessary action on the same it will work on its own once logs are created it will mimic the same action which a network admin would have done. RPA BOT will not only do the support part for IDS it will also save the efforts of network admins daily monotonous work which is necessary but time consuming.

IV. CONCLUSION

In this paper, we surveyed the list of existing intrusion detection system techniques. From the articles we found that intrusion attack detection problem is vigorous in nature and need refinement in models.

ISSN: 2233-7857 IJFGCN

We also found out that systems need automation as human intervention at some stages required which causes late incident response. We propose to develop an end to end IDPS leveraging RPA^3 technology with algorithmic refinements to defend databases against illegal intrusions.

We will present an empirical study on Automated IDPS for insider attack in a forthcoming paper. In upcoming article we will first start with the comparative analysis for the existing work. These methodologies will be studied and a suitable approach will be taken for further research. This will help us to get the appropriate approach to guide the research in right way to prevent the threats in a correct and reliable manner.

REFERENCES

[1] Mehul S. Raval, Ratnik Gandhi, and Sanjay Chaudhary," Insider Threat Detection: Machine Learning Way" Springer Nature Switzerland AG 2018
[2] Kaushal Bhavsar1 and Dr. Bhushan Trivedi. "Predicting Insider Threats by Behavioural Analysis using Deep Learning". Int'l Conf. Security and Management SAM'18 ISBN: 1-60132-488-X
[3] Souparnika Jayaprakash . Kamalanathan Kandasamy "Database Intrusion Detection System Using "Octraplet and Machine Learning". ISBN:978-1-5386-1974-2 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018.
[4] Raji Ramachandran, Nidhin R, Shogil P P," Anomaly Detection in Role Administered Relational Databases- A Novel Method" 978-1-5386-5314-2/18/ ©2018 IEEE
[5] Preeti Mishra, Vijay Varadharajan, Uday Tupakula, and Emmanuel Pilli, "A Detailed Investigation and Analysis of using Machine Learning Techniques for Intrusion Detection," In Proc. Of 2009 IEEE International Conference, IEEE COMMUNICATIONS SURVEYS & TUTORIALS 1553-877X (c) 2018 IEEE.
[6] Qussai Yaseen Aman Alabdulrazzaq Firas Albalas," A Framework for Insider Collusion Threat Prediction and Mitigation in Relational Databases" In Proc. of IEEE International Conference on Machine Learning and Cybernetics, 978-1-7281-0554-3/19/©2019 IEEE.

[7] Derui Ding, Qing-Long Han ∗, Yang Xiang, Xiaohua Ge, Xian-Ming Zhang," A survey on security control and attack detection for industrial cyber-physical systems" Springer Neurocomputing 275 (2018) 1674–1683.
[8] Hagit Grushka-Cohen, Oded Sofer, Bracha Shapira, Lior Rokach," CyberRank- Knowledge Elicitation for Risk Assessment of Database Security" ACM. ISBN 978-1-4503-4073-1/16/10.
[9] Drashti Nandasana Mr. Virendra Barot, "A Framework for Database Intrusion Detection System", I2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication 978-1-5090-0467-6/16 ©2016 IEEE.
[10] Kalyan Veeramachaneni CSAIL, MIT Cambridge, MA Ignacio Arnaldo. "AI2 : Training a big data machine to defend". 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), 978-1-5090-2403-2.
[11] Xiong Wen, Wang Cong. "Hybrid feature transformation based on modified particle swarm optimization and support vector machine". Journal of Beijing University of Posts and Telecommunications, 2009, 32(6): 24-28.
[12] LI Zhong-long, SI Jin. "Distributed Denial of Service Analysis". Computer Knowledge and Technology, 2010, 6 (6): 2373-2374.

[13] Xiang Xu ,Ding Wei , Yuelei Zhang. “Improved detection approach for DDOS attack based on SVM”, 2011, IEEE
[14] P. K. Agrawal , B. B. Gupta , Satbir Jain . “SVM Based scheme for Predicting Number of Zombies in a DDoS Attack” 978-0-7695-4406-9/11 $26.00 © 2011 IEEE
[15] Kashif Saghar , William Henderson ,David Kendall , Ahmed Bouridane , “Applying formal modeling to detect Dos attack in wireless medium”
[16] Xinfeng Ye , Santosh Singh “ A soa approach to counter ddos attack” 2007 IEEE
X`