ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

A Survey on Behaviour Based Intrusion Response System for Relational Database

Naresh Kamble, Pankaj Chandre

PG Scholar, M.E., Dept. of Computer Network, Flora Institute of Technology, Pune, India

Assistant Professor, Dept. of Computer Network, Flora Institute of Technology, Pune, India

ABSTRACT: Many approaches for dealing with intrusion in OS and Network have been proposed and worked on. But these methods may not be appropriate for a Database System. An anomaly detection system for relational databases is proposed. This work focuses on detecting anomalies in a particular database state that is represented by the data in the relations. Their first technique uses basic statistical functions to compare reference values for relation attributes being monitored for anomaly detection. The second technique introduces the concept of ¢ relations that record the history of changes of data values of monitored attributes between two runs of the anomaly detection system. This work focuses on the semantic aspects of the SQL queries by detecting anomalous database states as represented by the data in the relations, while we focus detecting anomalous access patterns in a DBMS.
Purpose of approach towards detection of abnormal accesses during info as painted by SQL queries submitted to the info. Associate degree anomaly detection system for relative databases is planned and social media posts for estimating people's reactions to communicated alert messages during crises. This work focuses on sleuthing anomalies during a specific info state that's painted by the info within the relations. Their initial technique uses basic applied math functions to match reference values for relation attributes being monitored for anomaly detection. The second technique introduces the construct of Δ relations that record the history of changes of information values of monitored attributes between 2 runs of the anomaly detection system. Another relevant approach towards a database-specific ID mechanism is by Hu et al. They propose mechanisms for locating knowledge dependency relationships among transactions and use this data to search out hidden anomalies within the information log.

KEYWORDS- Intrusion Detection (ID), Anomaly Detection (AD), Secondary Service Link Authenticator (SSLA), Joint Threshold Administration Model (JTAM)

I. INTRODUCTION

The key factors influencing how people react to and behave during a crisis is their digital or non-digital socialnetwork, and the information they receive through this network. Publicly available online social media sites make itpossible for crisis management organizations to use some of these experiences as input for their decision-making. During crises, enormous amounts of user generated content, including tweets, blog posts, and forum messages, are created, as documented in a number of recent publications. Undoubtedly, large portions of this user generated content mainly consist of noise with limited or no use to crisis responders, but some of the available information can also be used for detecting that an emergency event has taken place, understanding the scope of a crisis, or to find out details about a crisis. That is, parts of the data can be used for increasing the tactical situational awareness. Unfortunately, the flood of information that is broadcast is infeasible for people to effectively extract information from, organize, make sense of, and act upon without appropriate computer support recently, we have seen an interest in products that continuously monitor a database system and report any relevant suspicious activity. Database activity monitoring has been identified by Gartner research as one of the top five strategies that are crucial for reducing data leaks in organizations. Such step-up in data vigilance by organizations is partly driven by various US government regulations concerning data management such as SOX, PCI, GLBA, and HIPAA. Organizations have also come to realize that current attack techniques are more sophisticated, organized, and targeted than the broad-based hacking days of past. Often, it is the sensitive and proprietary data that is the real target of attackers. Also, with greater data integration, aggregation and disclosure, preventing data theft, from both inside and outside organizations, has become a major challenge. Standard database security mechanisms, such as access control, authentication, and encryption, are not of much help when it

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

comes to preventing data theft from insiders. Such threats have thus forced organizations to re-evaluate security strategies for their internal databases. Monitoring a database to detect potential intrusions, Intrusion Detection (ID), is a crucial technique that has to be part of any comprehensive security solution for high-assurance database security. Note that the ID systems that are developed must be tailored for a Database Management System (DBMS) since database-related attacks such as SQL injection and data ex filtration are not malicious for the underlying operating system or the network. Our approach to an ID mechanism consists of two main elements, specifically tailored to a DBMS: an Anomaly Detection (AD) system and an anomaly response system. We are using Secondary Service Link Authenticator SSLA which incorporates the user authentication info clearly explained in the proposed method. We follow the different types of response actions that we refer to, respectively, as conservative actions, fine-grained actions, and aggressive actions. A tainted request is marked as a potential suspicious request resulting in further monitoring of the user and possibly in the suspension or dropping of subsequent requests by the same user. The two main issues that we address in the context of such response policies are that of policy matching and policy administration. Policy matching is the problem of searching for policies applicable to an anomalous request. When an anomaly is detected, the response system must search through the policy database and find policies that match the anomaly.

Our mechanism is a real-time intrusion detection and response system; thus efficiency of the policy search procedure is crucial. Two efficient algorithms that take as input the anomalous request details, and search through the policy database to find the matching policies. We implement our policy matching scheme in the PostgreSQL DBMS, and discuss relevant implementation issues. We also report experimental results that show that our techniques are very efficient. The second issue that we address is that of administration of response policies. Intuitively, a response policy can be considered as a regular database object such as a table or a view. Privileges, such as create policy and drop policy that are specific to a policy object type can be defined to administer policies. However, a response policy object presents a different set of challenges than other database object types. Recall that a response policy is created to select a response action to be executed in the event of an anomalous request.

II. RELATED WORK

1. Purpose of study reviewed

Purpose of study is to know the traditional and existing approaches to Intrusion Response for Relational Databases, their advantages and limitations and to propose a system that will make use of the advantages and overcome the limitations. Proposed system makes use of the advantages of response system and overcome the disadvantages of existing approach.

2. Existing System Limitations

We tend to address in context of such response policies are that of policy matching, and policy administration. For the policy matching drawback, we tend to propose expeditiously search the policy information for policies that match an abnormal request. The experimental analysis shows that our techniques are terribly economical in order to protect information stored in a database.

2.1 Iterative or Evolutionary Model

2.2 Multihand Administration with Intrusion Avoidance in Database System

2.3 Security in Database Systems

2.4 Multihand Administration

2.5 HMAC

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

III. ARCHITECTURE

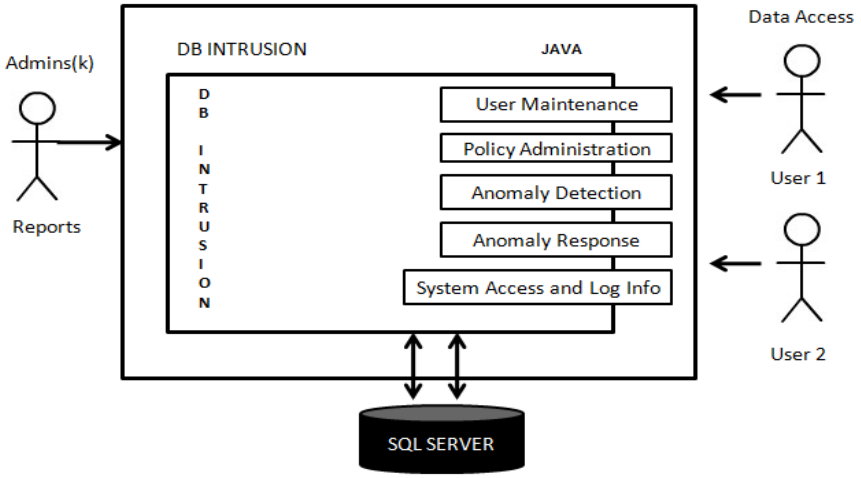

Fig 1. Block diagram of Intrusion Response System

It consists of three main phases:

1. Phase-1 or User Administration & Authentication
2. Phase-2 or H-K clustering process
3. Phase-3 or Split Process
4. Phase-4 or Ensemble clustering process

1. User Administration & Authentication

The DBA is centrally responsible for DB and user maintenance. By default there is only one DBA. The DBA then creates other DBA's and users. These users are maintained with appropriate privileges or permissions. Only these users can login and access the database objects.

2. Policy Administration

The main issue within the administration of response policies is the way to defend a policy from malicious modifications created by a DBA that has legitimate access rights to the policy object. To deal with this issue, we have a tendency to propose an administration model named JTAM.

3. Policy Activation

Once the policy has been created, it must be authorized for activation by at least k – 1 administrator after which the DBMS changes the state of the policy to ACTIVATED. An activated policy can be assigned to a user. A policy identifies the objects and privileges the assigned user has on the object.

4. Anomaly Detection

This part is predicated on the development of information access profiles of roles and users, and on the utilization of such Profiles for the AD task. A user request that doesn't adjust to the conventional access profiles is characterized as abnormal.

5. Anomaly Response System

This component is accountable of taking some actions once associate degree anomaly is detected. There are 3 main forms of response actions, that we tend to consult with, severally, as conservative actions, fine-grained actions, and aggressive actions

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

6. System log and access information

This module provides the DBA with anomalies detected and reports various activities or attempted activities made by the users. The DBA uses this to generate various reports based on which an action or the revoke of privileges are made.

IV. SYSTEM FLOW

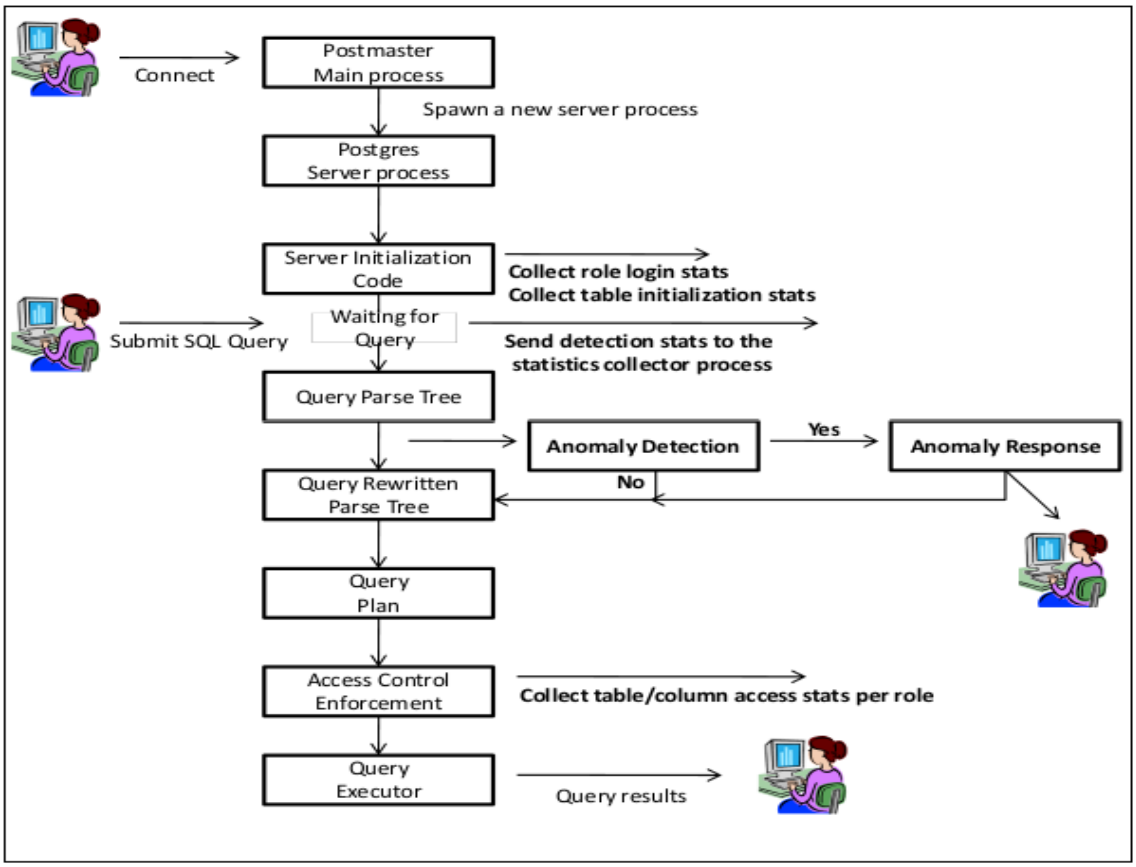

Fig.2 Flowchart of proposed model

Based on the above flowchart of proposed model, the following content will unfold these five sub-stages in details:

We have implemented our AD algorithm in the open-source DBMS PostgreSQL. Figure 1shows the query processing architecture and the application of our algorithm in the execution pipeline of a query.

For every new connection to the database, the main server process spawns a new server process called Postgres. Every SQL query sent on that connection is handled by this new Postgres process. When a new connection to the database is established by a user, we report the login statistics to the statistics collector process (server-side process) that includes the roles activated by the user, and the list of tables under AD. When the user submits a query, the query string passes through the query parser which creates a parse tree of the query structure. The parse tree is then modified by composing into it any *views* or *rules* that may apply to the query. This is performed by the query rewrite system. After the query has been rewritten, the query optimizer takes the parse tree and generates an optimal query plan that contains the operations to be executed for processing the query. The plan is then passed to the query executor that is responsible for executing of the query and passing the results back to the client. Before the executor begins executing the query, it checks whether the user has the privileges (directly or indirectly through role membership) to execute the query.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

V. PROPOSED MECHANISM

We propose a framework that uses a behavior-based white listing approach to learn normal behavior profiles and to detect deviations from such profiles as anomalies. Intuitively, if behavior profiles are built by combining query, result-set and context based features, it is possible to detect a wider set of data leakage threats. To this end, our approach builds profiles that encompass these different types of features. In addition, our approach is white-box in the sense that it allows the identification of the root causes of a data leakage and thus the quantification of its severity based on the sensitivity of the leaked in- formation. This makes it possible to prioritize alarms and therefore to reduce the impact of false positives. Furthermore, we intend to perform the detection of anomalies per set of and not per single query. This way, we can detect situations where a single query is not malicious, but n queries together are (e.g., T4) might be carried out by several small queries instead of a single one which might be more suspicious)

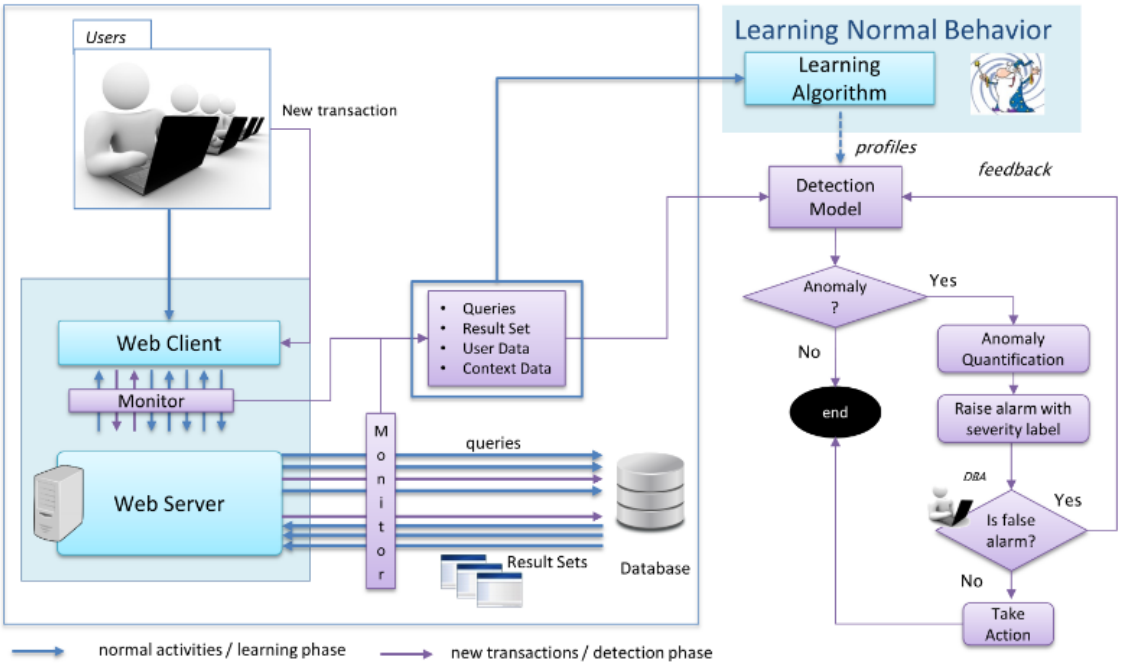

Fig.3 Detection Framework Description

VI. CONCLUSION

We have described the response component of our intrusion detection system for a DBMS. The response component is responsible for issuing a suitable response to an Anomalous user request. We proposed the notion of database response policies for specifying appropriate response actions. We presented an interactive Event-Condition-Action type response policy language that makes it very easy for the database security administrator to specify appropriate response actions for different circumstances depending upon the nature of the anomalous request. The two main issues that we addressed in the context of such response policies are policy matching, and policy administration. For the policy matching procedure, we described algorithms to efficiently search the policy database for policies matching an anomalous request assessment. We extended the PostgreSQL open-source DBMS to implement our methods. Specifically, we added support for new system catalogs to hold policy related data, implemented new SQL commands for the policy administration tasks, and integrated the policy matching code with the query processing subsystem of Postgre SQL. The experimental evaluation of our policy matching algorithms showed that our techniques are efficient. The other issue that we addressed is the administration of response policies to prevent malicious modifications to policy objects

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

from legitimate users. We proposed a JTAM, a novel administration model, based on Shoup's threshold cryptographic signature scheme. We presented the design and the implementation details of JTAM, and reported experimental results on the efficiency of the policy signature verification mechanism.

REFERENCES

1. Conry-Murray, "The Threat from within. Network Computing (Aug. 2005)," http://www.networkcomputing.com/showArticle. jhtml?articleID=166400792, July 2009.
2. R. Mogull, "Top Five Steps to Prevent Data Loss and Information Leaks. Gartner Research (July 2006)," http://www.gartner.com, 2010.
3. M. Nicolett and J. Wheatman, "Dam Technology Provides Monitoring and Analytics with Less Overhead. Gartner Research (Nov. 2007)," http://www.gartner.com, 2010.
4. R.B. Natan, Implementing Database Security and Auditing. Digital Press, 2005.
5. D. Brackney, T. Goan, A. Ott, and L. Martin, "The Cyber Enemy within ... Countering the Threat from Malicious Insiders," Proc. Ann. Computer Security Applications Conf. (ACSAC). pp. 346-347, 2004.
6. A. Kamra, E. Terzi, and E. Bertino, "Detecting Anomalous Access Patterns in Relational Databases," J. Very Large DataBases (VLDB), vol. 17, no. 5, pp. 1063-1077, 2008.
7. A. Kamra, E. Bertino, and R.V. Nehme, "Responding to Anomalous Database Requests," Secure Data Management, pp. 50- 66, Springer, 2008.
8. A. Kamra and E. Bertino, "Design and Implementation of SAACS: A State-Aware Access Control System," Proc. Ann. Computer Security Applications Conf. (ACSAC), 2009.
9. "Postgresql 8.3. The Postgresql Global Development Group," http://www.postgresql.org/, July 2008.
10. J. Widom and S. Ceri, Active Database Systems: Triggers and Rules for Advanced Database Processing. Morgan Kaufmann, 1995.
11. "Oracle Database Concepts 11g Release 1 (11.1)," http:// download.oracle.com/docs/cd/B28359_01/server.111/b28318/ datadict.htm, July 2009.
12. V. Shoup, "Practical Threshold Signatures," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), pp. 207-220, 2000.

BIOGRAPHY

Naresh A Kamble is a PG scholar in the Flora Institute of Technology, M.E. Computer Network Department, Pune, Pune University. He has received Bachelor of Information Technology (IT) degree in 2010 from Shivaji University Kolhapur, Maharashtra State, India and currently he is pursuing his Masters education in Computer Networks at Flora Institute of Technology, Pune in Pune University. His research interests are Information Security (Penetration testing), Big Data (Hadoop), Cloud Computing, Multimedia etc.

Pankaj R Chandre is an Asst. Prof. at Flora Institute of Technology in Computer Engineering Department, Pune, Pune University. He has received Master of Computer Engineering degree in 2011 from Mumbai University, Mumbai, India. His research interests are Information Security, Network Security, and Computer Networks etc.