Forensic Analysis of Database using Secure Audit Log

Shubhangi Kumbhar[1],Shital Garje[2], Runali Jadhav[3],V.N.Dhawas[4]

Department of Computer Engineering,
Sinhgad Institute of Technology,
Lonavala,Maharashtra,India

Abstract: **Database tampering is one of the big and important role in Database Management system. Database security is very important requirement of today's database application system. The Main Objective of this Paper is to identify different technique and detection of different contents in Database. Here we are using the cryptographic hash algorithm to detect the tampering of a Database. Consequently the Tiled Bitmap Forensic analysis algorithm helps to find at what time and possibly finally why and who had tampered the Database. Here we are using separate audit log validator to observe and inspect the database along with the extra information and state of the data. Audit log play a central role in database. A notarizer is used to create notary id of each hashed value of database transaction.**

***Keywords— Database security, database tampering, Audit log Manager, Notarizer , Digital Notarizer System, Validator*.**

I. INTRODUCTION

The United States Health Insurance Portability and Accountability Act (HIPAA) enable every patient to demand from their health care provider the name of every entity to whom her information has been revealed. For example, if a patient Alice receives advertisements for diabetes tests, she can check whether her health care provider has released the information that she is at risk of developing diabetes. In order to comply with HIPAA, the health care provider needs to maintain a tamper-proof audit log of all SQL queries issued to the system.The log can be used to identify all entities that accessed Alice’s health record. In order to provide such functionality when Alice makes such a request, a security admin has to analyze the audit log to check for queries that “accessed” Alice’s record.

The main focus of this paper is to destruct of database security threat and this threat can rise above during the Database Forensic and there is a huge amount of autonomous risk arise to store the more secret data into the database and there are many big organization are failure to inspect the data and data contravene. There are variety of risks create for the database security like Finance control, nature of threat. Lot of IT persons access the core database, limited number of Database security professionals.

II. RELATED WORK

Widespread news coverage of collusion between auditors and companies they audit, a recent FBI (federal Bureau of investigation) study shows that almost half of attacks done by insiders .It is assumed that the notarization and validation services remain in a trusted part of computing base. This can be done by making them geographically and perhaps organizationally separate from the DBMS and the database, so that finding out correct tamper detection even when the tampering is done by highly motivated insiders. Scenario, like discusses tampering event in which in U.S., all patients are required to sign an authorization under HIPAA .Computer forensics is now an active field, with more than50 books published in the last 10 years. There are few computer tools for these tasks, in part due to the heterogeneity of the data. One substantive example to show how computer tools can be used for forensic analysis is Mena’s book. Goodrich et al. introduce new techniques for using main-memory indexing structures for data forensics. We are using cryptographic hash functions to detect database tampering and of introducing additional hash chains to improve forensic analysis. Previously, there has been proposed the Monochromatic, RGB, and Polychromatic forensic analysis algorithms.

III. DIFFERENT FORENSIC PHASES OF DATABASE REGARDING TO THE TAMPERING

Authenticated and Authorized user access the data by using various mechanisms provided by the Database Server. But some time the authorized user makes the data get tampered, so the system is also not secured and protected.

Authorized user directly access the Database by using some legal act but authorized user also access the database with the help of IP address and try to make some modification in the database like changes in account balance or any customer related issue and this changes provides the financial loss that’s why Database server do not promise for the true data. Due to this issue we need the Forensic Analysis System. During the Digital Analysis of the Database number of operation is executed and Forensic Analysis will take care whether this operation is executed in sequential manner or not. The Forensic Analysis also collects the data during the analysis and operation execution and this data is needed to be submitted as evidence. Following Thing Need to be considered:

Data dictionary is the most important part and the target of the attacker need to make changes in Data Dictionary.

Data Dictionary also contains information, such as creation time of entity. The Forensic analysis algorithm using this information for the investigation.

During the forensic investigation number of users created number of different schemas and these schemas may relevant.

Audit log or Metadata or communication between this is use to find who is the authorized to perform certain action. Data mining tool provide valuable help in Forensic analysis algorithm.

IV. DATABASE TAMPER DETECTION PHASES

There are several things with database and ideas come with the database operation:

I] The First phase

Audit log maintain by the DBMS itself as a background. This background audit log representing individual relation and this individual relation is treated as a Transaction Time table. In DBMS we perform updating, Deletion and modification operation on data (Tuple) if this operation take long time the Audit log and Transaction time table Drill the DBMS to keep the previous tuple during this operation with their insertion and deletion/update time. During this The DBMS provide one important property with the stored Data in database that it is Modification. If want to modify the only add information at End no information is Deleted. If we change the old information that time the data get tampered.

II] The Second phase

The Transaction made the cryptographically hash for the modify data to generate the secure hash chain of Transaction.

III] The Third phase

With the use of external Digital notarization system we notarize the hash value because of this the intruder, operating system and hardware cannot change the hash value. If the intruder, operating system and hardware makes any Changes in hash value it is very difficult to make the hash value for this change hash value regarding to the Audit Log

IV] The Fourth phase

Finally the matching is performed between old hash values with rehash tuple. If hash value is same there is no problem but if matching is not occurred then we need to apply forensic analysis algorithm to find out where, when and why the tampering has been occurred.

V. PROPOSED MODEL

This model presents elements and the basic things regarding how to assemble the data and the security about this assemble data.

The different modules are as follows-

I] Audit Log Manager

Audit log maintain by the DBMS itself as a background. This background audit log representing individual relation and this individual relation is treated as a Transaction Time table. In DBMS we perform updating, Deletion and modification operation on data (Tuple) if this operation take long time the Audit log and Transaction time table Drill the DBMS to keep the previous tuple during this operation with their insertion and deletion/update time. During this The DBMS provide one important property with the stored Data in database that it is Modification. If want to modify the only add information at End no information is Deleted. If we change the old information that time the data get tampered.

II] DNS

DNS is the Digital Notarization System.Use an external notarization service to digitally notarize the hash data therefore, even if the intruder has access to everything (database, hardware, OS, etc) they cannot change the hash data. to digitally notarize this hash value with an external notarization service. So even if the intruder has full access to the database itself ,the DBMS, and even the operating system and hardware, the intruder cannot change the hash value. This makes it exceedingly difficult to make a series of changes to the audit log that generate the same hash value.

III] Validator

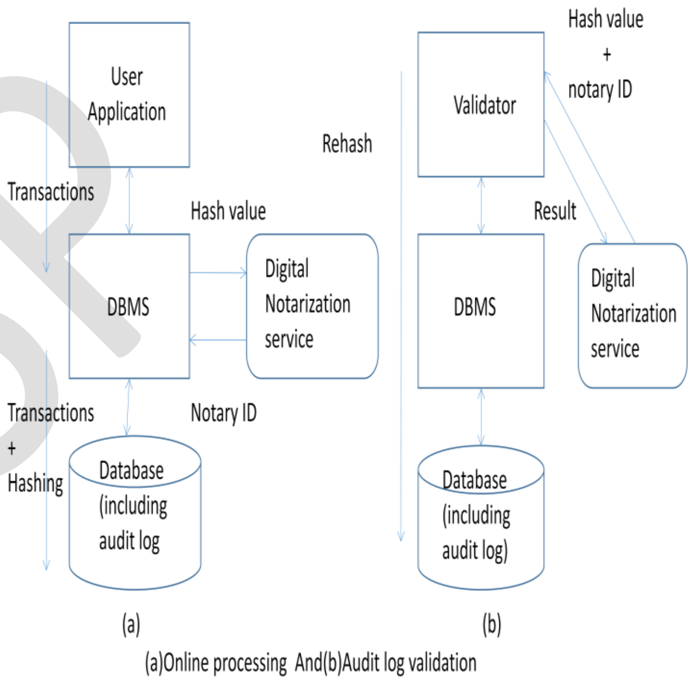
User Application
Transactions
DBMS
Hash value
Digital Notarization service
Notary ID
Transactions + Hashing
Database (including audit log
(a)
Rehash
Validator
Hash value + notary ID
Result
DBMS
Digital Notarization service
Database (including audit log)
(b)
(a)Online processing And(b)Audit log validation

Fig. Online Processing With Audit Log Validation

Finally the matching is performed between old hash values with rehash tuple. If hash value is same there is no problem but if matching is not occurred then we need to apply forensic analysis algorithm to find out where, when and why the tampering has been occurred.

VI. ADVANTAGES

1] To help as an evidence against the criminals.
2] To detect internal database frauds.
3] To help user to perform secure transactions.

4] Medical fields, companies, and government organization to guard their information from threats by applying this Enriched System .

VII. APPLICATIONS

1] Banks can use this system for secure transaction.
2] They can use the forensic report generted ass an evidence against criminals.
3] It will Help to detect frauds done by insiders.

VIII. CONCLUSION AND FUTURE WORK

Forensic analysis detects in what time a crime has been identify and in this case the tampering of a database. Such analysis activities determine when the tampering occurred, and what data were altered.

The present paper is concerned of only detecting the database tampering not about preventing tampering. The essential tools for auditing a database are in place and it is now possible for Medical fields, companies, and government organization to guard their information from threats by applying this Enriched System.

REFERENCES

[1] International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 2, February 2013) 439 Database Tampering and Detection of Data Fraud by Using the Forensic Scrutiny Technique Piyush P. Gawali1, Dr. Sunil R. Gupta2 Prof. Ram Meghe institute of technology & research, Amravati, Maharashtra, India.

[2] SELECT Triggers For Data Auditing Daniel Fabbri #1, Ravi Ramamurthy _2, Raghav Kaushik _3#Electrical Engineering & Computer Science, University of Michigan2260 Hayward Street, Ann Arbor MI 48109 USA1dfabbri@umich.edu_Microsoft Research One Microsoft Way, Redmond WA 98052 USA.

[3] Harmeet Kaur Khanuja, D.S. Adane , "DATABASE SECURIT THREATS AND CHALLANGES IN DATABASE FORENSIC:A SURVEY" 2011 International Conference on Advancement in Information technology with workshop of ICBMG 2011, Singapore IPCSIT vol. 20(2011),

[4] Harmeet Kaur Khanuja, D.S. Adane,"A FRAMEWORK FOR DATABASE FORENSIC ANALYSIS "Computer Science & Engineering : an International Journal(CSEIJ),vol.2,no.3,June 2012.