International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 2, February - 2014

Data Tampering Detection using the Tiled Bitmap Algorithm

[1.] Prashant Kamthe, [2.] Ketan Joshi ,[3.] Sanket Kale, [4.] Anjiri Ambadkar
[1,2,3,4.] Department of Computer Engineering
AISSMS Institute Of Information Technology
Pune, Maharashtra ,India

***Abstract*-Now a days database plays a very important role in almost every branch like medicine, computer science, business, administration, e-education, Science etc. Because of this, chances of data being tampered has gone up. So database security is the main concern of developers along with detecting the tampering in it .To deal with this issue various database forensic analysis techniques are available. In this paper we present an overview of two of them. Mainly one way hashed key algorithm and tiled bitmap algorithm.**

Cryptographically-strong hash functions can be used for Tamper Detection in database. Subsequently-applied forensic analysis algorithms can help determine when, what, and perhaps ultimately who and why. This paper presents a novel forensic analysis algorithm, the Tiled Bitmap Algorithm, which is more efficient than prior forensic analysis algorithms. It introduces the notion of a candidate set (all possible locations of detected tampering(s) and provides a complete characterization of the candidate set and its cardinality.

Keywords-Database Management, Security, integrity, database tampering, database forensic.

I. INTRODUCTION

Database is a well-organized collection of data. The data are typically organized to model relevant aspects of reality in a way supporting the processes requiring this information. Database management Systems (DBMS) are specially design applications that interact with the users, other applications and the database itself to capture and analyze the data.

In multi user database system, the DBMS must provide techniques to enable certain users or user groups to access selected portions of database restricting access to the rest of the database. This is particularly important when a large integrated database is to be used by many different users within the same organization, eg- sensitive info such as employee salaries or performance reviews should be kept confidential from most of the database system's users.

This section summarizes the tamper detectionapproach. There are several related ideas that inconcert allow tamper detection.

- The DBMS can maintain the audit log in the background, by interpreting a specified relation as a transaction-time table. This instructs the DBMS to retain previous tuples during update and deletion, along with their insertion and deletion/update time such that it is completely transparent to the user application. An important property of all data stored in the database is that it is append-only: modifications only add information; no information is ever deleted. Hence, if old information is changed in any way, tampering has occurred.
- The data modified (inserted/ updated/deleted) by a transaction can be cryptographically hashed to generate a secure one-way hash key of the transaction.
- Then digitally notarize this hash value. So even if the intruder has full access to the database itself, and even the operating system and hardware, the intruder cannot change the hash value. This makes it extremely difficult to make a series of changes to the audit log that generates the same hash value.

Their two executionphases: 1: Normal processing- In this phase the transactions arerun and hash values are digitally notarized. 2: Validation- The hash values are recomputedand compared with the previously notarized value. Tampering is detected during this phase, when thejust-computed hash value doesn't match the previously notarized value. Figure 1 illustrates these twophases.

Initially database is running fine, processing manytransactions per second. Periodically, it sends a hash value to the digitalnotarization service, receiving back a notarization IDthat it inserts into the hash sequence. At somevalidator will perform validation. The validator,reports that our database has been tampered. TheDBA and forensic analysis is initiated.

The validator provides a vital piece of information,that tampering has taken place, but doesn't offermuch else. Since the hash value is the accumulationof every transaction ever applied to the database,validator can't understand when the tamperingoccurred, or what portion of the audit log was corrupted.

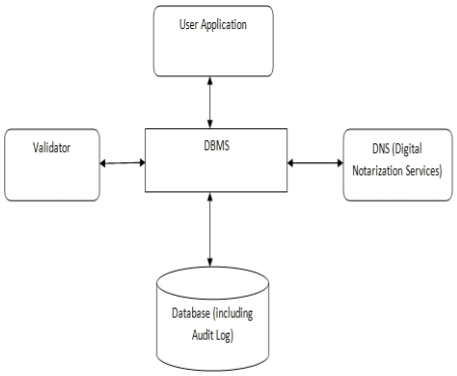

Figure 1: Validation and Notarization

II. RELATED WORKS

[1]A recent FBI survey implies that most of the attacks were supposedly to be done ny the inside people.
[2] Assumption is made that notarization n validation services remain trusted by making them physically separate from the database so that correct tamper detection is done .
[3] Kyriacos E. Pavlou and Richard T Snodgrass, Senior member, IEEE
In this paper the Monochromatic,the RGB and polychromatic Algorithms has been implemented. All these algorithms employ same approach of detecting the tampering , periodic validation and forensic anylysis but the main difference lies in the number of hash chains used.Also it shows that the existing algorithms are time consuming and slow in processing.
[4]Database Tampering Detection of Data Fraud by Using the Forensic Scrutiny Technique –Piyush .Gawali,Dr.Sunil.Gupta
In this paper RGBY ,A3D , RGB, Monochromatic and also Tiled bit map algorithm have been discussed. And a model is presented regarding the basic things like how to assemble the data and security about data.
[5]Improved Tiled Bitmap Forensic Analysis Algorithm-C.D.Badgujar, G.N.Dhanokar.
This paper discusses the existence of multi-locus corruption events can be better handled by summarizing the places of corruption using the candidate set,instead of try to use precision.
[6]In this paper ,malinda detcected the filed which is tampered, on this basic step, we are implementing and finding who did the tampering and where the tampering was done.

III. ALGORITHM

A. Hashed Key Algorithm :

B. MD-5:

MD5 (Message-Digest algorithm 5) is a well-known cryptographic hash function with a 128-bit resulting hash value. MD5 is widely used in security-related applications, and is also frequently used to check the integrity of files.
Accept string convert it into byte array .Accept a byte and convert it into hexadecimal and the OR with 0x100.

IV. THETILED BITMAP ALGORITHM

```
//st- start time
//it-interval time
//cv-current vector
//pv-previous vector
//dcv-data current vector
//dpv- data previous vector

TBA(it,cv,pv)
{
It=2min;
St=0;
If (compare cv and pv)
{
Check hash value;
}
For (i to cv.length())
If (cv[i] != pv[i])
{
Display Tamper Detection;
}
}
```

V. PROPOSED MODEL

This model presents elements and the basic things regarding how to assemble the data and the security about this assemble data.
Representation of Tamper Detection:
-A User will officially or unofficially create Tampering.
-That User Information stored in separate DW (Data warehouse).
-Validation Component provides Locking Mechanism and the Locking mechanism LOCK the all secured collected Audit Logs.

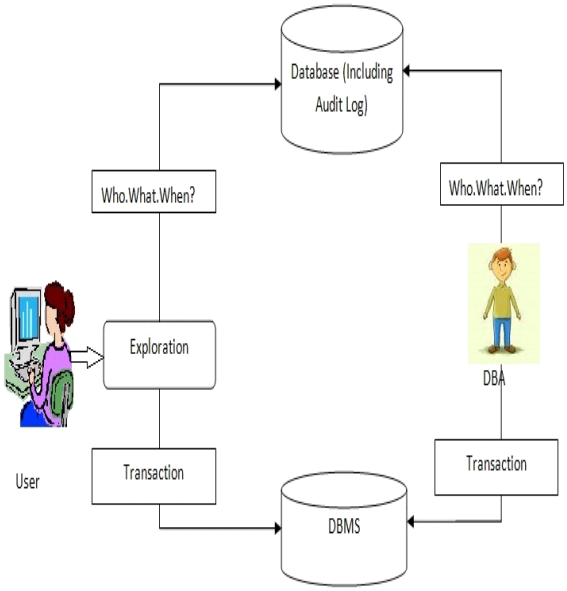

Figure 2 : Tamper Detection

-By using the SQL we perform different operation (INSERT, UPDATE, and DELETE) in database. If modification wants to perform, this modification happens in background of the Database. User plays with this operation and modification by using the certain application, so the user request goes through the application layer and call the SQL to execute the procedure of operations.

- During INSERT operation into Audi table, trigger evaluates two hash values and stores with every record. Figure 3 describes this mechanism in more details [16].The submission of request goes to the DATABASE by using the SQL, as discuss above the submission of request goes through the application layer is not the last fragment of Information system or the DBMS.After the submission the detection is generated with the SQL prompt. Prompt is the schedule of encoding of program and this prompt assign with the event and the SQL prompt implemented in special SQL code. The SQL prompt executed automatically. DDL prompt is also one important part in RDBMS, some of DDL prompt is specially bunch together and make the group of this special DDL Prompt. In RDBMS the Database objects is created, if someone wants to make any changes in database that time the DDL prompt is executed.

- There are two special columns called HReserved and VReserved as shown in Figure 3 below. The algorithm involving these two columns are in a way that whenever there is an insert operation in the Audit Log table two hash values - a row hash, and a column hash of this table is calculated. The final Fragment is the security, and each and every record pass through the last fragment.

VI. (EXPECTED) ANALYSES AND RESULTS

It introduce the parties involved and the underlying threat model.The parties involved are:

- The DBMS.
- An external digital notarization service. This is a company which can digitally notarize documents and then validate their correctness.
- The validator. This is a DBMS application which periodically contacts the digital notarization service.
- The forensic analyzer. This is a DBMS application responsible for executing the chosen forensic analysis algorithm.

The algorithm now recomputes the other four partial hash chains for this tile, c1-c4. Four partial hash chains are used to get down to an hour granularity, given that each tile is 16 hours, which is the validation time.

Sr.No	Name	Date and Time	Data Field
1	Radheya	15/12/2013,02:25PM	Book
2	Gurmeet	18/12/2013,10:25PM	Discount
3	ketan	21/12/2013,12:25PM	Salary
4	sandeep	02/01/2013,03:25PM	Book Price

Figure 3 : Result Table

VII. CONCLUSION

Due to centralized storage of data notarization and validation becomes easier .The paper suggest the advanced methods for detection of tampering.And overcoming the previous proposals that included only the field detection, Who tampered the data and where the change was made is implemented.Along with this restoration of the tampered data is also done.To make storage of data and data handling safer.

REFERENCES

[1] "The tiled bitmap forensic analysis algorithm", K.E. Pavlou and R.T. Snodgrass, IEEE transaction on knowledge and data engineering, Vol. 22, pp no.590-601, April 2010.

[2] CSI/FBI, "Tenth Annual Computer Crime and Security Survey," http://www.cppe.um.edu/Book store/Documents/2005CSISurvey.pdf, 2009.

[3] "An Infrastructure for Database Tamper Detection and Forensic Analysis", M. Malmgren, honors thesis, Univ. of Arizona, 2009.

[4] U.S. Dept. of Health & Human Services, The Health Insurance Portability and Accountability Act (HIPAA), http://www.cms.hhs. Gov/HIPAAGenInfo/, 2009.

[5] "Tamper Detection in Audit Logs", R.T. Snodgrass, S.S. Yao, and C. Collberg, Proc. Int'l Conf. Very Large Databases, pp. 504-515, Sept. 2004.

[6] "Forensic Analysis of Database Tampering", K.E. Pavlou and R.T. Snodgrass, ACM Trans. Database Systems, vol. 33, no. 4, pp. 1-47, Nov. 2008.