IJETAE
EXPLORING RESEARCH AND INNOVATIONS

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)

Database Tampering and Detection of Data Fraud by Using the Forensic Scrutiny Technique

Piyush P. Gawali[1], Dr. Sunil R. Gupta[2]

Prof. Ram meghe institute of technology & research, Amravati, Maharashtra, India

***Abstract*— Database Tampering and the Data Fiddle is one of the important role in Database Management System (DBMS).To Provide the security to the Data Storage Has Become Requirement of our time. The Main Objective of this Paper identifies different technique and detection of different Places in Database. We are using the cryptographic hash algorithm to discover the tampering of a Database. Consequently the Tiled Bitmap Forensic analysis algorithm helps to find at what time and possibly finally who and why Tamper the Database. This algorithm establish the concept of applicant places (possible places of spot tampering) and prevent the intruder, the computing of the candidate set is also presented.**

The separate audit log validates to observe and inspect the database along with the extra information and state of the data. Audit log play a central role in database. The space and time complexity is less in this forensic analysis algorithm.

***Keywords*— Database security, database tampering, logs and database forensic, Database Management, integrity and protection, temporal databases, Effective Notarize, Validator.**

I. INTRODUCTION

The appropriate current central laws (i.e. federal laws) HIPAAACT [12] (Health Insurance Portability and Accountability), PIPEDA Canada act and the involvement of prevalent news among the assessor and the companies they audit (e.g., Enron, WorldCom) helped to hasten current passage of federal laws and authorized improved control on electronic data and The submissive record are those necessaries by the numberless laws and the regulations. This laws and regulation help to maintained, stored, created and preserved the Data.

The main focal point 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.

Cryptographically strong one-way hash functions agree to the finding of a corruption event (CE), which is several event that violate the data and conciliation of database.

Due to enemy as well as auditor or employee or even unfamiliar bug in software, or hardware crash corruption event occurs [10].

II. RELATED WORK

Widespread news coverage of collusion between auditors and companies they audit [1], a recent FBI study indicates that almost half of attacks were by insiders [2].It is assumed that the notarization and validation services remain in a trusted computing base. This can be done by making them geographically and perhaps organizationally separate from the DBMS and the database [3], thereby effecting 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 [4].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 of how computer tools can be used for forensic analysis is Mena's book [5]. Goodrich et al. introduce new techniques for using main-memory indexing structures for data forensics[6].In the database context, previous papers introduced the approach of using cryptographic hash functions to detect database tampering [7] and of introducing additional hash chains to improve forensic analysis [7]. Previously, there has been proposed the Monochromatic, RGB, and Polychromatic forensic analysis algorithms [8].

If an adversary modifies even single byte of data or its timestamp, the independent Validator will detect mismatch with the notarized document, thereby detecting the tampering. The adversary could simply re-execute transactions, making whatever changes he/she wanted, and then replace original database with his/her altered one. However, the notarized document would not match in time. Avoiding tamper detection comes down to inverting the cryptographically strong one way hash function. An extensive presentation of an approach, performance limitations, tamper detection, threat model and other forensic analysis algorithms is discussed in paper[7],[9].

المنارة للاستشارات

www.manaraa.com

Hash chain linking is discussed in more detail in paper[7]. Tiled bitmap algorithm is refinement of polychromatic algorithm. The advantage of the Tiled Bitmap Algorithm is that it lays down a regular pattern (a “tile”) of such chains over contiguous segments of the database. The other advantage of the Tiled Bitmap Algorithm is that it can detect multiple corruption events that other previous algorithms can-not. On the other hand it suffers from false positives while the previous algorithms do not. There are many models have been proposed to find the tamper detection process like

A) Monochromatic Algorithm

The Monochromatic Algorithm uses only the cumulative (black) hash chains we have seen so far, and as such it is the simplest algorithm in terms of implementation.

B) RGB Algorithm

In the RGB Algorithm, three new types’ chains are added, denoted with the colors red, green, and blue, to the original (black) chain in the so-called Monochromatic Algorithm. These hash chains can be computed in parallel; all consist of linked sequences of hash values of individual transactions in commit order. While additional hash values must be computed, no additional disk reads are required. The additional processing is entirely in main memory. The RGBY Algorithm retains the red, green, and blue chains and adds a yellow chain.

C) RGBY Algorithm

The RGBY Algorithm is an improvement of the original RGB Algorithm. The main insight of the previously presented Red-Green-Blue forensic analysis algorithm (or simply, the RGB Algorithm) is that during notarization events, in addition to reconstructing the entire hash chain (Illustrated with the long right-pointed arrows in prior corruption diagrams), the Validator can also rehash portions of the database and notarize those values, separately from the full chain.

D) A3D Algorithm

The a3D Algorithm is the most advanced algorithm in the sense that it does not lay repeatedly a “fixed” pattern of hash chains over the database. Instead, the lengths of the partial hash chains change (decrease or increase) as the transaction time increases, in such as way so that at each point in time a complete binary tree (or forest) of hash chains exists on top of the database. This enables forensic analysis to be speed up significantly. In all the above mentioned algorithms they differ in the amount of work necessary during normal processing.

AS we seen in Monochromatic algorithm we use an array Black Chains of Boolean values to store the results of validation during forensic analysis. Computing additional hash chains during periodic validation) and the precision of the when and what estimates produced by forensic analysis. The Boolean results are indexed by the subscript of the notarization event considered: the result of validating is stored at a given index. Since we do not wish to pre compute all this information, the validation results are Computed lazily, i.e., whenever needed. This can give rise to corruption easily. The RGBY Algorithm was designed so that it attempts to find more than one Corruption Event. However, the main disadvantage of the algorithm is that it cannot distinguish between three contiguous corruptions and two corruptions with an intervening notarization interval between them. The a3D Algorithm is working on the recursive pattern for the call of notarization service. Where if the Chain is having lager tree then it performs faster but fails to get desired result for all the intervals.

E) Tiled Bitmap Algorithm

This algorithm 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. An optimal algorithm for computing the candidate set is also presented. Finally, the implementation of the Tiled Bitmap Algorithm is discussed, along with comparison to other forensic algorithms in terms of space/time complexity and cost. Where candidate Set Function is to arrange values of targeted binary array in reverse order and renumber function is to re arrange values of targeted binary array imperfect order. So in our proposed System the DBMS computes a cryptographically strong one-way hash function for each tuple inserted and then notarizes it using a notarization service. This made it possible to check the consistency of the data by comparing it to the values stored with the notarization service. In continuation with this method, algorithms were designed to further analyze an intrusion of database.

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.

المنارة للاستشارات
www.manaraa.com

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 item price and changes in item quantity 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 Algorithm. The authorized and unauthorized user detected by the Tiled Bitmap forensic analysis algorithm [10].

The Forensic Analysis method is logically planned. 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 subtle 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. TAMPER DETECTION APPROACH

With the Database there are several things and ideas come with the database operation.

The First approach: 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.

The Second approach: The Transaction made the cryptographically hash for the modify data to generate the secure one-way hash of Transaction.

The Third approach: By using the external notarization service 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

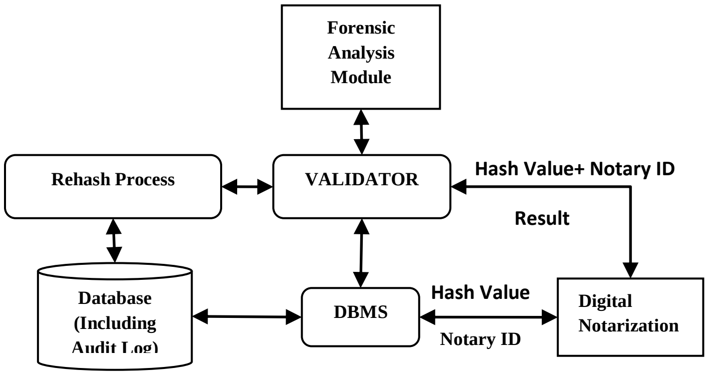


Fig 1: Online Processing with audit log validation

*The Fourth Approach***:** 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.

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.

المنارة للاستشارات
www.manaraa.com

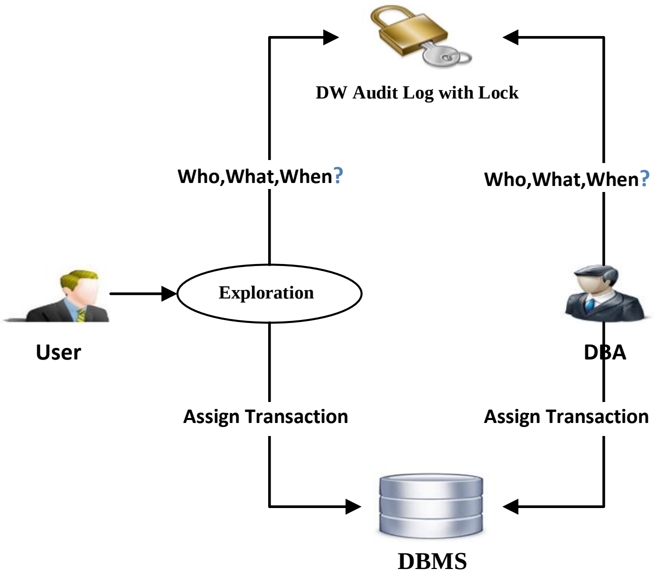


Fig 2: Tamper Detection Model

-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.

The last fragment is created with the cryptographically one way hashing function to provide the hash value for each every individual row. This Fragment is also used for the storing the audit log so when we want to enter data into the audit table the cryptographic method and triggers generate the two values, one value for the ROW and another value for COLUMN. We know that the table in database is nothing but the collection of ROWS and COLUMNS. For each and every individual ROW we are using separate column and the name of this column is HReserved (HR) and another separate column for each and every individual column and name of this column is VReserved(VR).The row is stored in HR and this HR contain hash value for all column without including HR and VR if we want to change the data available in a ROW or if we want to modify the data available ROW, so this modification or change provide new hash value so mismatch Is performed Within old hash value and new hash value and the tampering is detected. The CV contain column hash value, and this hash value based on RV.IF the intruder delete a row form the audit table the algorithm find a mismatch by the continuation of new two rows immediately foregoing the deleted row.

The tiled bitmap algorithm [13] is the modified version of the polychromatic algorithm [15], the group of a sequence

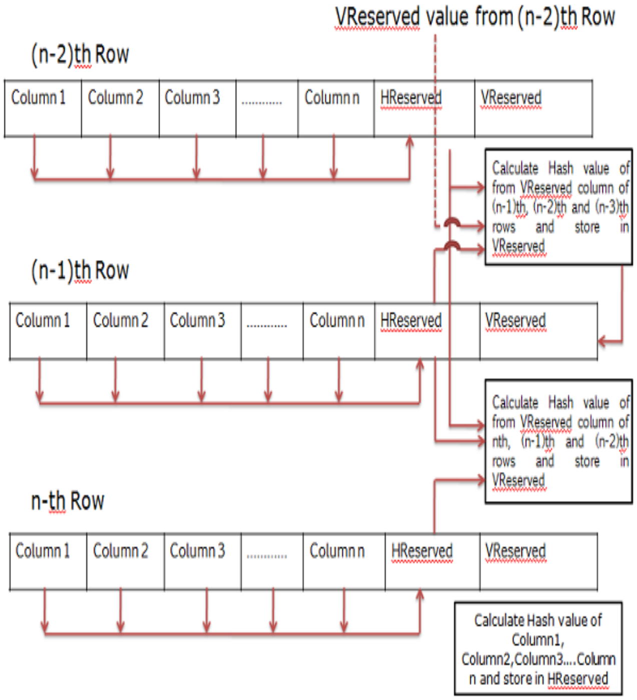
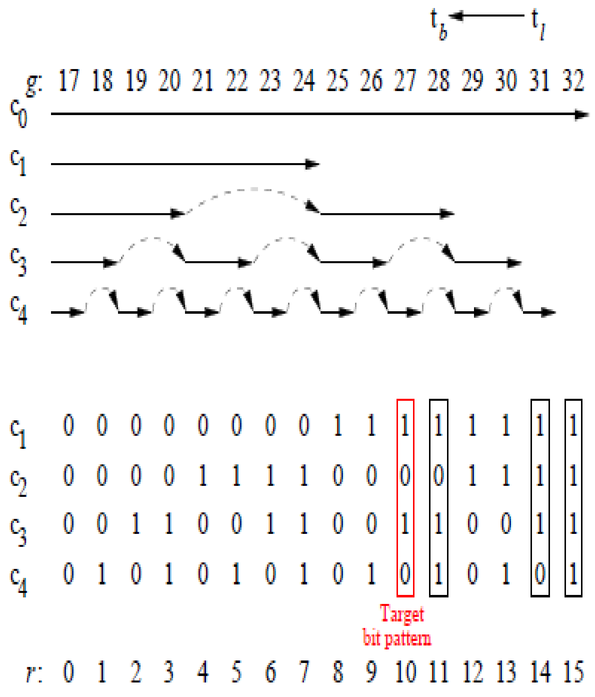

VReserved value from (n-2)th Row
(n-2)th Row
Column 1
Column 2
Column 3
....
Column n
HReserved
VReserved
Calculate Hash value of from VReserved column of (n-1)th, (n-2)th and (n-3)th rows and store in VReserved
(n-1)th Row
Column 1
Column 2
Column 3
....
Column n
HReserved
VReserved
Calculate Hash value of from VReserved column of nth, (n-1)th and (n-2)th rows and store in VReserved
n-th Row
Column 1
Column 2
Column 3
....
Column n
HReserved
VReserved
Calculate Hash value of Column1, Column2,Column3....Column n and store in HReserved

Fig 3: Audit Log Protection Mechanism

المنارة للاستشارات
www.manaraa.com

Value (hash chain) and there is some time gap between these hashes chain and this hash chain coupled with this time gap and real validation interval. Below figure 4 shows the validation happens every 16 hours, during this time thousand even millions of transaction occur, and below figure 4 shows one 16-hour fragment (slice).time proceed from left to right with the hour shown as r = 0 to r = 15 and in second fragment hour 17 match up with r = 0 an hour 28 match up with r = 11 and below figure4 also demonstrate a corruption event and in this corruption event the timestamp of tuple relation was changed from 31 to 28 hour. consider this relation contain confidential information and when this confidential information discharge authorization were sign by the patient, in this case authorization was sign in hour 31.an hour 29 a doctor expose the patient health information to insurance company and he recognize his mistake, actually this is the crime under act of HIPAA[1].by using the left pointing arrow on hour 28 the authorization backdated and database entail that the authorization received before confidential information convey.



c_1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
c_2	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
c_3	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
c_4	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
r:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Fig 4: Hash Chain

The forensic analysis algorithm hamper the corruption event and also restrict the corruption within the every hour, as shown in figure 4 there are five hash chain is available from c0 through c4.

The c0 has chain hashes all transaction with the notarization interval of 16 hour and c1 hash chain hashes the transaction only for the first 8 hour, c4 hash chain hashes the other hour transaction. The dotted line indicates the communication of hash chains. as shown in figure 4 in the hash chain c4the last transaction hash value of hour 0 hashed with the first transaction of hour 2[5].For the tamper detection after some hour all hash chain are recomputed on tampered data and this recomputed value send to the notarize server, the server find the matching between the old and new hash value if matching is found there is no tampering in data and unmatched value shows the tampering is occurred.

By using the forensic analysis algorithm the hash chain c0 report during the 16 hour the tampering is occurred The remaining four chain compute the 4-bit value based on the corruption event and this 4 bit value is 1010.the c1 hash chain value and c3 hash chain value is not affected by the corruption but hash chain value for c2 and c4 is not matching with previous value. the truth value as shown in figure 4 the target string would result had the corruption event tampered with the data stored at the indicated hour and also the timestamp changed from tl to tb from 31 to 28 and corruption event occurred at hour 47 .In forensic analysis algorithm the our targeted binary value is 1010.changing the data of 1 hour of interval make all of chain as a failure.

The target 1010 indicates the several possibilities.

-The first possibilities is the only the data in hour 27 was modified(r=10).

-The second possibilities is the timestamp move from 28 to 31(r=11 to r=14).

-The third possibilities are the timestamp move from 31 to 28.

-The fourth possibilities are the change from hour 27 to 31, a change from 32 to 27.

A) Proposed method

In this section, we describe our approach of Tamper Detection and Forensic Analysis according to the steps shown in figure 2

There are 13 main steps available in our approach.

Step 1, 2, and 3: In This step's the DBA (Database Administrator) give permission to client for the Database Operation, This client's digital signature is created by using the SHA-1 algorithm with the DSA.This signature is in encrypted form.

Step 4, 5 and 6: In these steps we upload both the master data on which operations need to be performed & also a digital signature.

للاستشارات المنارة
www.manaraa.com

When Client want to perform any operation regarding to Database with refer to master database that time the client digital signature is verified. The Client signature and master database data stored in a specific location of the web server of DW (data ware house).The Audit Log is also provided with the Data warehouse.

Step 7: As shown in figure 1 The Client and DBA Assign Transaction to the DBMS Then all the data field enter Through the Web application. The separate uploading panel provides to the clients and the DBA and these panels temporally stored in java bean classes.

Step 8: Through the Administrator the digital signature is uploaded in Data warehouse and this is act as notarize element for each and every transactions, whenever the transactions occurs notarize confirm the private key for those Transactions. If private key is same as provided by the Administrator then the transaction completed successfully otherwise the transaction rejected.

Step 9: The Validate conveys the transaction details to notarize, by using these details notarize authorize the data.

Step 10: After the Data confirmation through the Validator, the strong cryptographically one way hashing is performed on this data with the MD5 Algorithm which gives a sixteen byte hash value for both the master data & also for the transaction data either by the auditor or by the organization employee.

Step 11 and 12: In this step the hash value is check in between the master data and transaction data if value is same there is no tampering is occurred but if the hash value is different in between the master and transaction data then the MD5 algorithm check whether this un matching produce a very large amount effect on dataset in this way we are going to detect data tampering for the several data owner for their own data with their respective applications with their respective signature.

*Step 13:*In this step the forensic analysis performed on each and every individual tampered tuple to find who tampered the data, what time tampering has been has been occurred and the field where tampering has been happened.

Here in our projected algorithm it admit Master data set and transaction data set after that we produce a one more set called Dset which truly consists of array of data field index whose value will be setting to begin with "0". This specifies that the fields are not yet tampered. Then for each master data set Mset and for each transaction data set Tset our algorithm capture each data fields of these two sets and match up both of them. If they are not equal then that data field is considered as tampered and then di that belongs to Dset is set to value "1".

This way the complete tuple is continue checking for the correct tampered fields and tampered person name can be discover using servlet which actually set the user name as he/ she login into the system and by using date and time operation on the same case we can calculate the accurately at time data tampering is been occur.

We propose the above Discussed Forensic Analysis method by using following Algorithm:

```
// input: //MDs set is the set of master database
// Mdh Master Database Hash Value
// TDs is the set of Transaction database
// Tdh Transaction Database Hash Value
// Dset is the set of Data Field Index
//Ne Notarize Element
// UN is Username
//Dsign Digital Signature by using SHA-1Treated as a Private Key
// td is date and time
// Rset is the set of Result
// output: Rset the set of Result
Function forensic Analysis (MDs, TDs, Dset, UN, td, Rset)
1: ClientDsign Created (Private Key)
2: For Each transaction
        If Dsign is same
            {Assign Transaction}
Else {Denies Transaction}
3: di =0 // data field Index
 4: Initially Result Set Empty Rset=""
5: for i= 1 to number of data fields
6: Tdh Transaction Database Hash Value
7: Mdh Master Database Hash Value
8: ifTdh! =Mdh
9: di =1
10: end of for
11: for i= 1 to number of data fields
12: if di =1
13: Rset = Rset + di
14:ReturnRset-
```

VI. Estimation And Methodology

7.1 Time Complexity of Forensic Analysis Algorithms

The Monochromatic Running time complexity is O (log(D/Iv)),RGB Running Time complexity is O(D/Iv),Tiled bitmap running time complexity is O((D.Ig Iv)/Iv+D).The Polychromatic algorithm is not here because it is exchanged with the tiled Bitmap Algorithm beside with our approach. With the time our algorithm is gradually slower because of the Chain enlargement and the use of this enlarge chain in our algorithm. As compare to our approach the Monochromatic is fastest one but this algorithm identify only the first corruption event.

المنارة للاستشارات
www.manaraa.com

The Tiled Bitmap Algorithm is somewhat extent in improved manner, this algorithm retain the enlarge chain of Monochromatic algorithm and this algorithm order the corrupted tiles by executing the binary search. This Modification not disturb the asymptotic Running time. Our algorithm is very time consuming because we will find the corruption event on each and every transaction.
So Time Complexity of our algorithm is: O (log (D/Iv))

7.2 Space Complexity of Forensic Analysis Algorithms:

The Space complexity of Monochromatic and RGB Algorithm is O (D) but for the suitable validation interval IV the space complexity is cost is higher. In Tiled bitmap algorithm the cost for this validation interval IV is smaller but in our approach the cost for this validation interval IV is smaller as compare to Tiled Bitmap algorithm. This cost also affects the space complexity of forensic analysis algorithm.

Space Complexity of Tiled Bitmap Algorithm (D. (1+lg IV)/IV).

Space Complexity :(D. (log IV)/IV).

7.3 Invention Scrutiny:

The Tiled Bitmap Algorithm [1] recommended that the tamper detection complete only for the tiles but in our approach we perform the tamper detection on live data. In our approach Master Database is strong and regimented to sustain the structure and also communicate with the all tools available in system. For the Future scope this Database simply expandable.

This Algorithm gives a systematic path to the employee and auditor for the secure communication with the system. By using this algorithm we stop the database disturbance form insider's and the outsider's. Because of the audit log it is capably auditing the central database.

Table 1
Result

Sr.No.	Person Name	Date & Time	Data Field
1	Piyush	15/01/2013,01:23 PM	Author Name
2	Shraddha	16/01/2013,03:45 PM	Discount
3	Sais	17/01/2013,04:00 PM	Discount

VII. Conclusion And Future Work

Forensic analysis inaugurate sat 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 develops upon that work by present the Tiled Bitmap Algorithm which is cheaper and more commanding than previous algorithms. This algorithm utilizes a logarithmic number of hash chains within each tile to narrow down the when and what and Checking the hash chain values create a binary number; it is the task of the algorithm to compute the pre image of bitwise We also note that previous algorithms do not handle multiple corruption events well, whereas the Tiled Bitmap Algorithm can separately examine corruption events occurring both in different tiles and several corruption events happening within a single tile and By creating a central database for all of the tools in the system to cooperate with it made it possible for the notarize and Validator to execute their action effectively. They can now stock up their data in this central database as fine as use the in sequence stored in it to plan future implementation. 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] CSI/FBI, "Tenth Annual Computer Crime and Security Survey,"July2005,http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf (accessed April 16, 2009).

[2] P. A. Gerr, B. Babineau, and P. C. Gordon, "Compliance: the effect on information management and the storage industry, "Enterprise Storage GroupTechnicalReport,May2003,http://www.enterprisestrategygroup.com/ESGPublications/ReportDetail.asp?ReportID=201 (accessed April 21, 2009).

[3] M. T. Goodrich, M. J. Atallah, and R. Tamassia, "Indexing Information for Data Forensics," in Proceedings of the Conference on Applied Cryptography and Network Security, Springer Lecture Notes in Computer Science 3531, pp. 206–221, 2005.

[4] B. Li, M. S. Hsiao, and S. Sheng, "A Novel SAT All-Solutions Solver for Efficient Pre image Computation," in Proceedings of the IEEE International Conference on Design, Automation and Test in Europe, Volume 1, February 2004.

[5] M. Malmgren, "An Infrastructure for Database Tamper Detection and Forensic Analysis" Honors Thesis, University ofArizona, May2007. http://www.cs.arizona.edu/projects/tau/tbdb/MelindaMalmgrenThesis.pdf(accessed March 27, 2009).

[6] J. Mena, Investigative Data Mining for Security and Criminal Detection, Butterworth Heinemann, 2003.

[7] K. E. Pavlou and R. T. Snodgrass, "Forensic Analysis of Database Tampering," in Proceedings of the ACM SIGMOD International Conference on Management of Data, pp. 109–120, Chicago, June, 2006.

[8] K. E. Pavlou and R. T. Snodgrass, "Forensic Analysis of Database Tampering," ACM Transactions on Database Systems33 (4): Article 30, 47+25 pages, November 2008.

المنارة للاستشارات
www.manaraa.com

[9] S. Sheng and M. S. Hsiao, "Efficient Pre image Computation Using A Novel Success-Driven ATPG," in Proceedings of the IEEE International Conference on Design, Automation and Test in Europe, Volume 1, March 2003.

[10] R. T. Snodgrass, S. S. Yao, and C. Collberg, "Tamper Detection in Audit Logs," in Proceedings of the International Conference on Very Large Databases, pp. 504–515, Toronto, Canada, September 2004.

[11] C. Strachey, "Bitwise operations," Communications of the ACM4 (3):146, March 1961.

[12] U.S. Dept. of Health & Human Services, The Health Insurance Portability and Accountability Act (HIPAA), 1996, http://www.cms.hhs.gov/HIPAAGenInfo/ (accessed April 16, 2009).

[13] U.S. Public Law No. 107-204, 116 Stat. 745.The Public Company Accounting Reform and Investor Protection Act, 2002.

[14] K. E. Pavlou and R. T. Snodgrass (2010, April).The Tiled Bitmap Forensic Analysis Algorithm. IEEE Transactions on Knowledge and Data Engineering, 22(4):590-601.

[15] "Forensic Analysis of Database Tampering", K.E. Pavlou and R.T.Snodgrass, Proc. ACM SIGMOD Int'l Conf. Management of Data, pp. 109-120, June 2006.

[16] Amit Basu, Article on Forensic Tamper Detection is SQL Server Tables, http://www.sqlsecurity.com

المنارة للاستشارات
www.manaraa.com