International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 03 | Mar -2017 www.irjet.net p-ISSN: 2395-0072

Survey on An effective database tampering system with veriable computation and incremental updates

Prof. Sanjay B.Waykar[1], Manisha S.Devkar[2], Pooja V.Gore[3] , Archana A.Kambire[4]

[1] *Professor, Dept. of Computer Engineering, Sinhgad Institute of Technology, Lonavala Maharashtra, India*
[2 3 4] *Student, Dept. of Computer Engineering, Sinhgad Institute of Technology, Lonavala, Maharashtra, India*

Abstract - *From the previous few years the use of databases has increased exponentially. Almost all of applications in world's largest organizations use database to manage their data. Huge numbers of database security breaches are occurring at a very high rate on daily basis. Now a days attack that occurs in companies are not only by outsiders but also by insiders. Insider may perform illegal action & try to hide illegal action. Companies would like to be assured that such illegal action i.e. tampering has not occurred, or if it does, it should be fastly discovered. Mechanisms now exist that discover tampering of a database, through the use of cryptographically-solid hash functions. Forensic analysis algorithms are used to detect who, when, and what data had been tampered. The Tiled Bitmap Algorithm, which is more efficient than previous forensic analysis algorithms. Tiled Bitmap Algorithm introduces the idea of a candidate set and provides a complete characterization of the candidate set and its cardinality. Existing Tiled bitmap algorithm can find out the possible combination of candidate set. It is unclear to get exact information about tampering from the candidate set as it contains false positives. Tiled Bitmap Algorithm is discussed; along with a contrast to previous forensic algorithms. The improved algorithm will be able to find out exact information about tampered data.*

Key Words: **Verifiable Database, Incremental Cryptography, Outsourcing Computations, Vector Commitment.**

1. INTRODUCTION

As the web is accesible over the every corner of the world it is crowded by the users like never before. So, the expanding number of online users alarmingly raises the data in the database through their web applications. In the many domains the data is becoming so huge in every minute and it is also important to protect it from the inside attackers of the storage organizations. Areas like telecom, banking and online shopping are heavily relay on systems which are protecting the data.

There are some methodologies like Bilinear pairing, verifiable database,Tiled Bitmap etc. through which we can see the assessment of present day database alter recognition framework. As tampering events are growing day by day, there is a need to have some mechanism by way of which either such events can be detected or prevention measures can be taken. Finding out regions of tampering give necessary clues to find out who have done that tampering. Illegal tampering may causes an organization very adverse effect during an auditing. **N**ow forensic analysis is an active field. Our aim is to focus on tamper detection and instance of tampering.

1.1 TEMPER DETECTION APPROCH

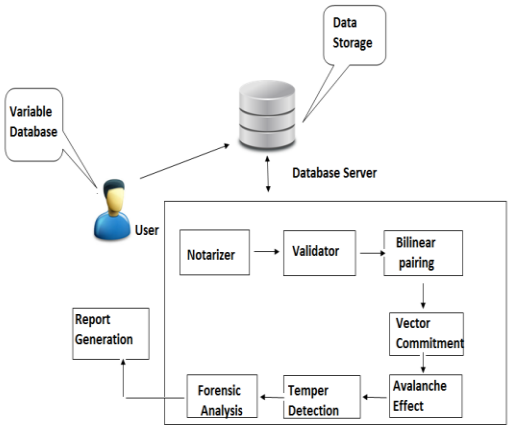

Fig-1. Audit log validation (Online Processing)

The essential approach separates two enforcement phases: online processing, in which transactions are run and hash esteems are digitally notarized, and validation, in which the hash esteems are recalculated and compared with those already notarized. At the time of validation that tampering is detected, when the just-calculated hash esteem doesn't match those already notarized. The two enforcement phases assign together the natural processing phases as opposed to the forensic analysis phase. Fig. demonstrates the two phases of typical processing.

In Fig. the client application performs transactions on the database, which add, remove and upgrade the rows of the present state. In the background, the DBMS keeps up the audit log by rendering a predetermined relation as a transaction-time table. A digital notarization service [1]is used that, when provided with a digital document, provides a notary ID. Later, at the time of audit log validation, the notarization service can determine, when presented with supposedly unchanged document and the notary ID, whether that document was notarized, and if so, when. On each change of a tuple, the DBMS acquires timestamp, calculates a

cryptographically[6] solid one-way hash function of the (new) data in the tuple and the timestamp, and sends that hash esteem, as a digital document, to the notarization service, obtaining a notary ID. The DBMS stores that ID in the tuple. Later, an interloper gets access to the database. If he changes the data or a timestamp, the ID will now be conflicting with whatever remains of the tuple. The interloper cannot change the data or timestamp so that the ID remains legitimate, because the hash function is one-way. Take note of that, this holds even when the interloper has access to the hash function itself. He can rather process another hash esteem for the changed tuple, but that hash esteem won't coordinate the one that was notarized. An autonomous audit log validation service later sweeps the database (represented in Fig), hashes the data and the timestamp of each tuple, provides it with the ID to the notarization service, which then checks the notarization time with the saved timestamp. The validation service then reports whether the database and the audit log are compatible. If not, either or both have been traded off.

1.2 FORENSIC ANALYSIS APPROACH

In this step once the data tuple is considered as tampered then the forensic analysis operation[7] is performed on this tuple to discover who is the person tampered the data, when is tampering happened and what are the correct field where tampering happened. Here in our proposed algorithm it accepts Master data set and transaction data set then we create a another set called D_{set} which really consists of array of data field index whose value will be setting initially as "0". This indicates that the fields are not yet tampered.

Then for each master data set M_{set} and for each transaction data set T_{set} our algorithm takes each data fields of these two sets and compare both of them. If they are not equal then that data field is considered as tampered and then d_i that belongs to $D_{se\ t}$is set to value "1". This way the complete tuple is keep checking for the correct tampered fields. Then this array of tampered fields is rearranged and also checking for more granularities to print the outcome.

The tampered person name can be identify using servlet which actually set the client name as he/ she login into the system and by utilizing date and time operation on a similar instance we can compute the exactly at time data tampering is been happened.

2. LITERATURE SURVEY

1.Illustrates the concept of Bilinear Pairing[3] can be used to reduce a hard problem in one group to a different, usually easier problem in another group.but it only checks one bit of record at a time only so it requires more time.

2.Discusses a concept of verifiable database (VDB) [5]enables a resource-constrained client to safely outsource a very large database to an untrusted server so that it could later retrieve a database record and update a record by allocating a new value. It is having drawback of it doesn't support public veriability (i.e., only the owner of the database can verify the correctness of the proofs).

3. Narrates the concept of Avalanche Effect checks the hash esteem of the master data & the transaction data. If the avalanche affect produces any positive changes then we consider there is some tampering is been happened at the transaction data then we note that data set as an infected one or a tampered one. In this way we are going to detect the data tampering for the numerous data owners for their respective data with the separate applications with their respective signatures. But, Avalanche Effect refers to a desirable property of cryptographic algorithms where, if an input is changed slightly (for example, flipping a single bit) the output changes significantly so it requires more time.

4.Introduce the concept of Vector Commitment (VCs)[2]allow to focus on ordered sequence of q values (m1,...,mq) in such a way that one can later open the commitment at specific positions (e.g., prove that mi is the i-th committed message). For security, Vector Commitments are required to fulfill a notion that we call position binding which express that an adversary should not be able to open a commitment to two different values at the same position.It is having drawback of schemes assumed that the size of the outsourced database should be fixed and the client can know the outsourcing function in advance.

5.Explain the concept of Hashing[6] which utilizes hash function tries to find collision. It exhibits the notion of incremental cryptography to outline cryptographic algorithms whose output can be upgraded very efficiently when the underlying input change.it is having disadvantage that client only needs to recompute the ciphertext on this certain block and the ciphertext of other blocks remains identical.

6.Describe the concept of non-interactive verifiable computation[4].Though the solution permits a client to outsource the calculation of an arbitrary function.it is having disadvantage that it is inefficient for practical applications due to the complicated fully homomorphic encryption (FHE) techniques.

3. CONCLUSION

Owners of web applications and data owners generally outsource the task of storing databases at the third party side. As this process may take high financial and security burden. But there is always a question of trust worthiness of the third party is there due to complex and huge infrastructure of data warehouses. So to secure the databases from any kind of interloper (mostly internal) a secure system is required to analyze after intrusion effect and perform the proper recovery steps. So this paper eventually studies the effect of different database tampering

system and tries to explore the facts and flaws of the system. So by analyzing all , this paper comes to a conclusion of requirement of strong and multi layered secured system for proper tamper detection and data recovery process on the same instance of interloper.

REFERENCES

[1] "The Tiled Bitmap Forensic Analysis Algorithm", Kyriacos E. Pavlou and Richard T. Snodgrass, Senior Member, IEEE transactions on knowledge and data engineering, vol. 22, no. 4, april 2010.

[2]"Vector Commitments and their Applications", D. Catalano and D. Fiore, PKC 2013, LNCS 7778, Springer-Verlag, pp.55-72, 2013.

[3] "Accumulators from bilinear pairings and applications", L. Nguyen, CT-RSA 2005, LNCS 3376, Springer, pp.75-292, 2005.

[4] "Non-interactive verifiable computing: Outsourcing computation to untrusted workers", R. Gennaro, C. Gentry, and B. Parno, CRYPTO 2010, LNCS 6223, Springer, pp.465-482, 2010

[5] "Verifiable delegation of computation over large datasets", Advances in Cryptology, S. Benabbas, R. Gennaro, and Y. Vahlis, CRYPTO 2011, LNCS 6841, Springer, pp.111-131, 2011.

[6] "Incremental cryptography: The case of hashing and signing", Advances in Cryptology, M. Bellare, O. Goldreich, and S. Goldwasser, -CRYPTO 1994, LNCS 2836, pp.216-233, SpringerVerlag, 1994.

[7] "Enriching Forensic Analysis process for Tampered Data in Database" ,Pallavi D Abhonkar, Ashok Kanthe International Journal of Computer Science and Information Technologies, Vol. 3 (5) , 2012,5078-5085.