International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 9 5634 - 5637

Development of Surveillance Technique on Database for Forensic Analysis

Swati Purohit
ME Scholar,
Dept. of Computer Science,
Jodhpur National University,
Jodhpur.

Dr. Rajesh Purohit,
Associate Professor,
Dept. of Computer Science,
J.N.V University,
Jodhpur.

1. Introduction

In this digital era technology is has broaden its roots from our table tops to laptops and now all handheld gadgets from research institute to common house hold work. Due to expansion of digital world, expansion of databases can also be observed very easily. With large volume of data comes the big issue of security.A layman to an enterprise its very crucial to maintain high data security. Like other areas forensic to trace the tampering activity of data.

Surveillance plays a vital role in forensic analysis, whether it is network forensics or database forensics. Due to preservation of data at different places traces are also observed or seen at different places in .Advance surveillance technique helps in recording the changes at different place. Due to multiple traces it is easy to track the tampering and evidence collection can be preceded easily.

2. Database forensics science

According to standard definition of database forensic "it isa branch of forensic science related to database and its Meta data" [1]. Paul wright is pioneer of database forensic specialised in Oracle [2]. In this paper we propose a prototype developed for surveillance technique for databases. Main aim is to develop this technique to provide security with resource present in Database management system. Many forensic algorithms are present which are used to detect tampering of data but no algorithm or prototype is present which can just notify that an event has been occurred. The resources that are used in this technique are storedprocedure, functions, triggers, programmed events, checksums which are already present in database system. By arranging all the above resources a surveillance technique can be made. This helps every user to maintain security on its own without a help of third party. So breaching of other party is not possible. Database forensic is an important part of digital forensics. As any department had to deal with data and maintain database. Database forensics has its approach to every department. As we are talking about forensic science on data base it is very necessary to know how a forensic analysis takes place.

Forensic analysis of database: Forensic analysis is upright event of tampering that has been done.It can only be observed that a data or entry has been affected. Preliminary step that is habitually taken is checking the log file. But after observing the log file we have found out no trace can be found out what and where data has been tampered. It just shows when which user has logged in and from where. The only trace which we can find. According to Law related [3] to digital forensic proceedings can only be held when a sufficient number evidence can be trace .Next equalling the data with backup which makes backup susceptible to be harmed. What if we develop a forensic copy rather than backup copy? Forensic copy and backup copy is widely different from each other on basis of theiruse [4].Forensic analysis means collection of evidence from number of location [3] [4] [5]. According to Harmeet kaur and D.S Adane forensic analysis is logical and carefully planned order of operation that are executed[5].Even in some database system an audit log is preserved however only in some so have to progress it for our sake [5][6][7][8].Some of the database forensics are given below:

1. Relation between data dictionary and conceptual layer because mostly data dictionary is target of intruder
2. During forensic analysis all views should be considered
3. The external scheme tells about the specific user
4. Check whether checkpoint has been deleted or reset

3. Methodology.

As our mainaim is to develop a technique which can keep surveillance over database and kind of forensic copy may be created.

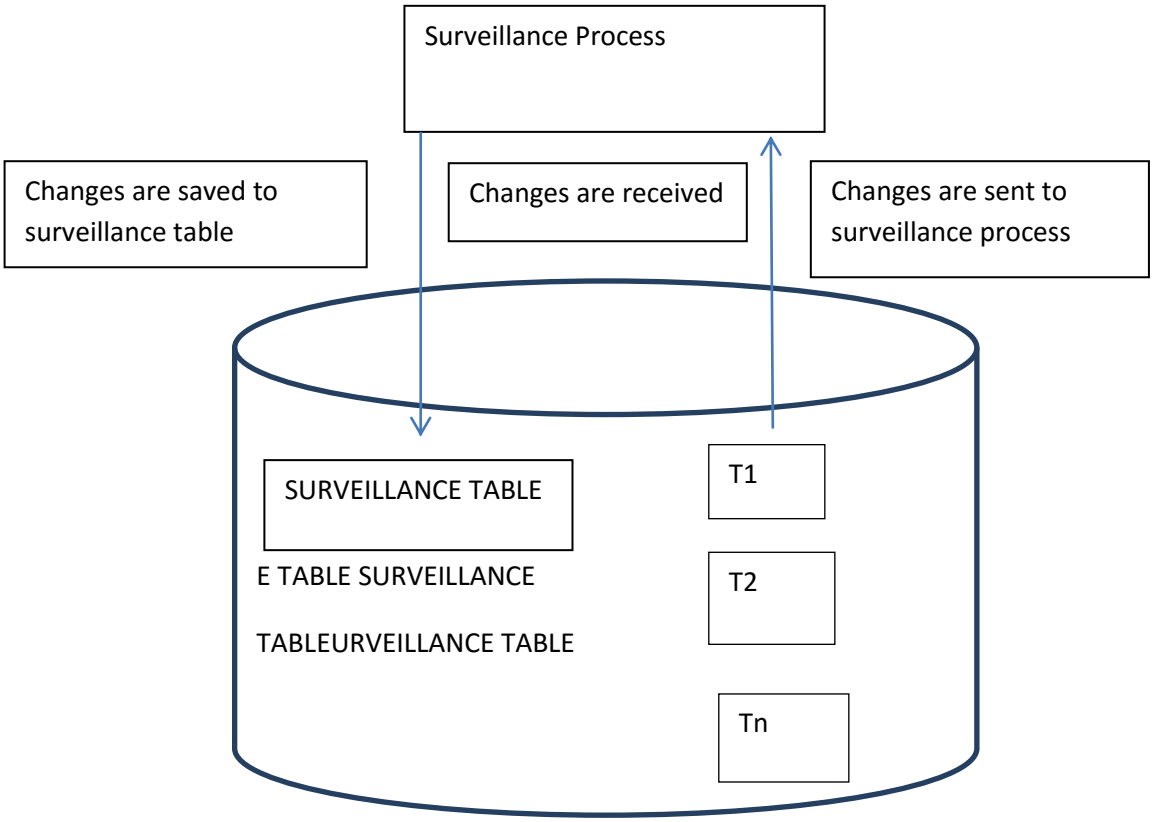
Procedure: whenever a database table is created thenits surveillance table can be created at the same time. This surveillance table should contain all values and details of the main database table. Creating identical table is need so that data entering of data should not change its format. Additional columns are added which stores *timestamp, action, revision.*

Timestamp: when did the data got entered

Action: what action has been taken like add, delete, update

Revision: what action has been performed for how much time it has been changed.

A block diagram for surveillance technique:



Preliminary Phase:It is an initial diagram where data is being saved in surveillance table. For saving data in another table at every enter or updating. Triggers are created and scheduled at on event. Changes made are saved in surveillance table with the action that means which trigger was fired. e.g. if user inserts the data in main table then changes made, s.no, time, revision that how many times data has been changed and the value of whole table is triggered and saved in surveillance table and it is same for all the others action performed.

Event full Phase:Every table have a unique number that gets changed after bring up to date, deletion or insertion and that number is known as *CHECKSUM* value of table.Definition according to Wikipedia"A checksum is a count of the number bits in transmission unit that is included with unit and so". If one keeps record of all checksum time to time then it can be observed when checksum was changed.

Checksum is a kind of function which calculates transmission bits. If a user develops a user defined checksum function for its individual table and record it then, Tampering will not only be a rigorous process but can be more specific.

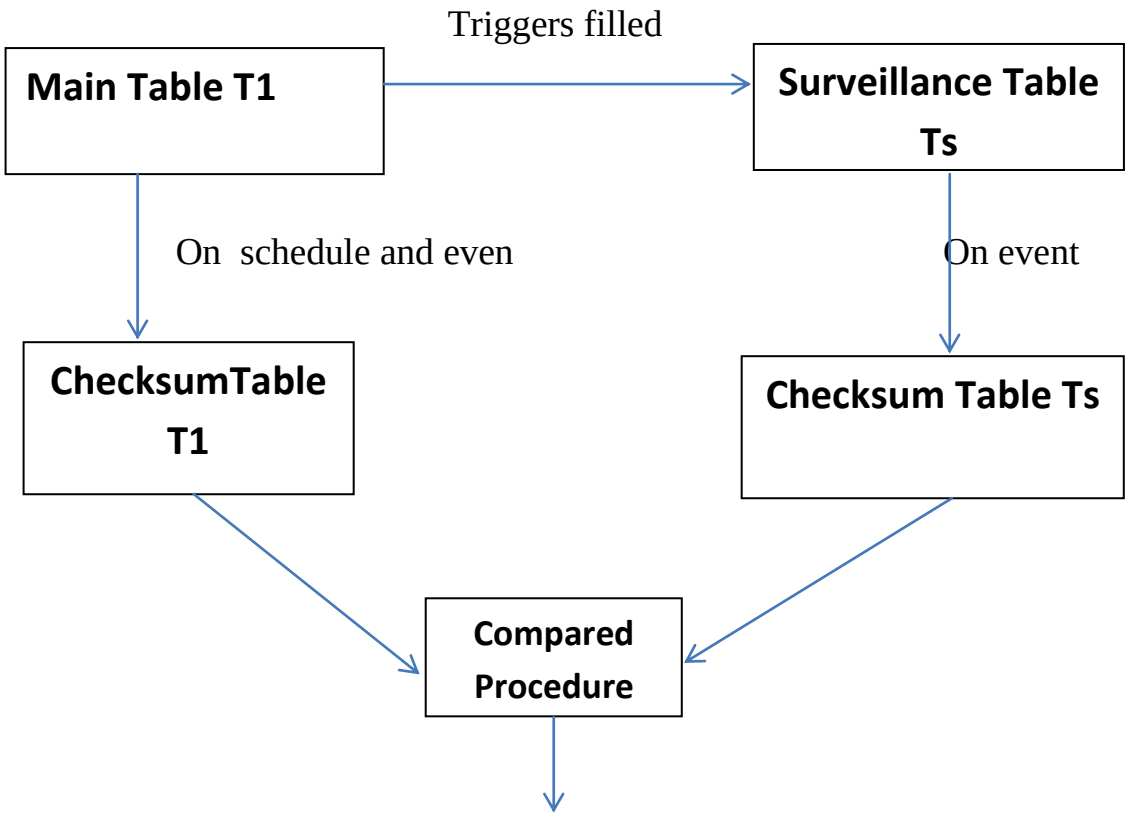
Comparison Phase: In this phase a comparison has to be made in checksum record of main table to checksum record of surveillance table. This comparison will be made on the basis of time. If one finds the changes on the basis of time i.e. if a change in one is recorded all other three tables then comparison will be successful and tampering could be detected. Here a user has to develop a procedure or a function to compare table on the basis of time.

Evidence Collection phase: The whole application revolves around forensics. It's time to collect evidences:

1) If changes is observed in main table but not in others than tampering is done
2) If checksum value is being changed continuously of any one table then tampering is being done
3) If log file show no authenticated user is logged in and changes are observed then tampering has been done
4) If surveillance table shows all data of one entity and main table doesn't or some queries are delete then tampering can be observed

All the processes are independent none of the resource and action is dependent on each other. Triggers and events work independently.

Block diagram for the surveillance technique phase wise



4. Conclusion:

A technique is developed with help of triggers procedure, function and user defined function for surveillance technique on database for forensic analysis

References:

1. Wikipedia *"DATABASE FORENSICS"*
2. "*Database forensics*" by Mario A.M Guimares Richard Austin Huwaid said.
3. "*Computer forensics InfoSec pro guide* " by Tata McGraw Hill
4. "*Digital evidence for database tampering*" by swhetha tripathi, fr. angel college ,Navi Mumbai and BanduBaburaomash ram by technological institute 2012
5. "*Forensic investigation for database tampering using audit log*"by Mrs .Prof. Jadhav sheetal, Miss borikar utkarsha sudhir,Miss kardil bhagyashree, Mrs aphale madhuri sudam.
6. "*Database tampering and detecting database fraud by forensic scrutiny technique*" Prof. Piyush p Gawali , Prof Ram Meghe institute of technology& research ,Amravati , Maharashtra , India, 2011

7. "*forensic tool and biometric* " by LeuteleLucia Mary grey, 2011
8. "*Database security threats and challenges in Database forensic* "by Harmeet kaur januja and D.s Adane ,Asst. prof pune, March 2015
9. R.T Snodgrass, S.S Yao, C.collberg "*tamper detection audit log*".
10. K.E.Pavlou and R.T Snodgrass "*Tiled bitmap forensic algorithm*" IEEE April 2011
11. "*Threat to privacy in forensic Analysis of database system*",Patrick Stahlberg, Giraomi micklao, dept. computer science,University of Massachusetts.