e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

DATABASE TAMPER DETECTION SYSTEM THROUGH TILED BITMAP ALGORITHM

Sneha Yendhe[*1], Shravani Pingat[*2], Sayali Ukirde[*3], Pooja Mandale[*4], Mr. V.V. Jadhav[*5]

[*1,2,3,4]Department Of Computer Engineering, Jaihind Polytechnic, Kuran, Pune, Maharashtra, India.

[*5]Guide Department Of Computer Engineering, Jaihind Polytechnic, Kuran, Pune, Maharashtra, India.

ABSTRACT

The Database has been one of the most effective forms of storing massive amount of data. The amount of data being generated nowadays has been increasing every day. The conventional and the most effective forms of storing the have been through the use of Relational Database Management Systems. The RDBMS allows for efficient management and storage of the data which is used by majority of the corporations and organizations across the globe. These databases are then targeted by attackers to gain unauthorized access which can be a highly problematic for everyone involved. Therefore, a collection of related research papers has been analyzed to achieve the effective solution for improving the security and maintaining the integrity of the database. This research report outlines an effective and useful realization of the improved security in Relational Databases through forensic analysis using Bilinear Pairing, distributed blockchain framework and avalanche effect detection.

Keywords: Database Integrity, Bilinear Pairing, Avalanche Effect, Validation Notarization, Blockchain.

I. INTRODUCTION

One of the earliest tasks undertaken by humans is information collecting and preservation. Humans have a history of accumulating data over time in order to transfer on their expertise to subsequent generations. This information can be immensely important in realizing the civilization' overall growth. Knowledge has permitted enhanced information that may be valuable in supporting community development, making it one of the pillars of human advancement. Our forefathers' expertise has equipped us to better our present ways, and the gathered expertise has culminated in global growth acceleration.

This information was presented in the form of drawings, with the majority of exchanges taking place by word of mouth. The cave drawings were primarily intended to teach future and emerging hunter gatherers about the technique and art of predation. This was modified when language emerged and huge volumes of data were handed down the generations by word of mouth. This resulted in considerably faster expansion, leading to the present day, when massive volumes of data are created and disseminated all over the world.

Data is essential to our existence and data processing in the everyday life. Database forensics is a discipline of research that studies databases and the in-formation that goes with them. This field uses standard forensic procedures and techniques to investigate database contents and metadata. Everything we see, as well as what we may conceive, can be saved as original data. This gathered information may be utilized for a variety of objectives, such as obtaining information about a person's checking account or learning about a family's or individual's health information. All of this information is kept in separate databases. We will need some sort of database management solution to adequately manage all of the information. The Database Management System is what these are labeled. These technologies not only assist us in effectively storing and retrieving data, but also in securing our records.

Relational database management has been progressively prevalent because it allows for more reliable and efficient data management. The information is recorded in the RDBMS in the table format, each of which has some type of link between both the data's different properties. Individuals, as well as big enterprises and organizations throughout the world, store the majority of their information in this manner. Because the information in these databases might be useful to attackers, they are objectives of assaults and other breaches.

The intruders exploit the premise that all of the essential and secret data is housed in a specific location that can be attacked to accomplish their malicious objectives. This is amongst the most successful and often used attacks that involves breaking into databases in order to obtain access, thieve, and modify information. This was among the most serious issues that many firms confront, as their clients' secret and private information is

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

at risk, putting the entire corporation in jeopardy. As a result, an effective strategy that can safeguard and maintain the stability of the RDBMS is required.

The various researches have been thoroughly analyzed for its merits and de-merits to help conceptualize our approach for the purpose of maintaining the integrity of the database and restoring the original database after an intrusion. The blockchain approach has been one of the most effective as per the analysis which has been crucial for the development of the methodology due to the tamper-proof nature of the approach. The blockchain approach has been one of the most effective and useful methodologies that have been emerged in the recent years.

The blockchain allows for the storage of information in a highly effective format which contains the data as well as the respective hash keys. The hash keys are useful in determination of any changes to the data which will trigger an avalanche effect that will be indicative of some tampering or modification. The approach has been detailed in the subsequent sections of the research article with effective quantification through extensive experimentation.

II. METHODOLOGY

Problem Statement

To enhance the process of database tampering proposed methodology put forwards an idea of detecting tampering attack on databases using Bilinear pairing and Blockchain technique which is powered with avalanche effect of the hash codes of data tuples in regular intervals. System not only detects all the details of forensics and also it clearly restores the original database.

III. MODELING AND ANALYSIS

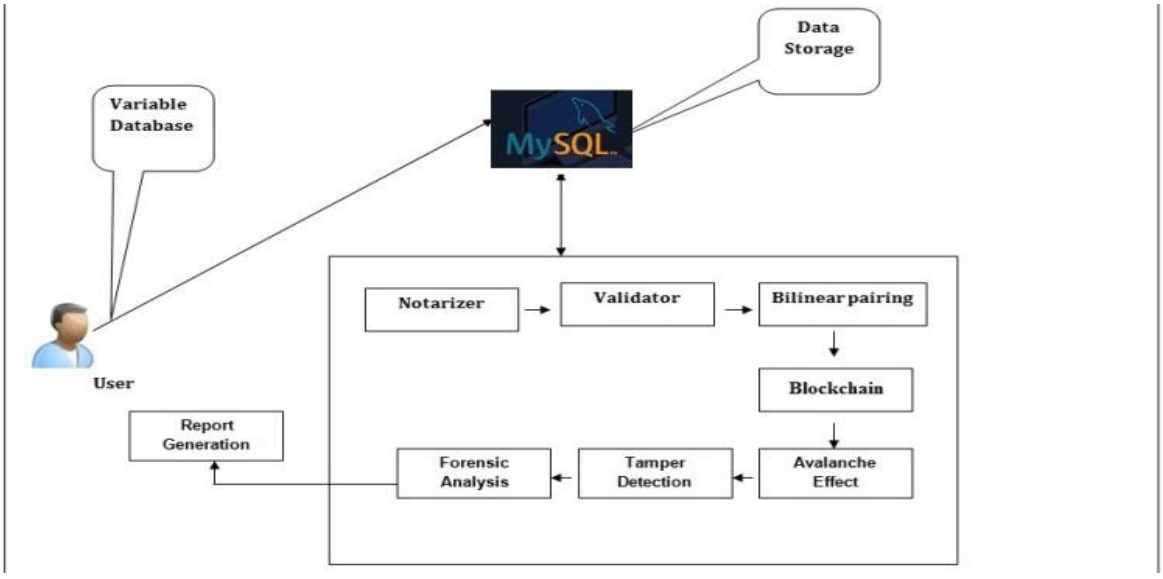

Figure 1: System Overview Design

The proposed methodology of variable database integrity maintenance system can be depicted with its step in figure 1. And these steps are deeply narrated in the below mentioned steps.

Step1: Notarizer - This is the very first step, Where each and every database client who is willing to store the database at the third party organization are getting a unique notarization key based on their attributes. This key is being generated by the random selection of seven characters through MD5 hash key, which is generated by the client's attributes. And this key is helping to authenticate the client while he is uploading the data to the cloud.

Step 2: Validator - Once the data is stored in the third party servers, then a validation of the data is started for the stated period, Like it may be 1,2,3,or 60 minute period. Here in each validation time a current and previous data vectors are maintained to get the Tamper Detection results.

Step 3: Bilinear Pairing and Avalanche Effect - This is the Core part of the system where, for the given validation time a pair of hash keys are generated for the each and every database tuples and they are referred as the

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

bilinear pairs. These bilinear pairs are compared for the integrity loss of the database tuples. A change in the single bit of the data tuples yields the massive change in the hash key, Which is referred as the Avalanche effect.

This Avalanche effect helps to identify whether the database tuples are tampered or not. If the data base tuples are tampered then the primary key of the tuples are extracted as tampered ID . This ID eventually represents the which tuples are being targeted by the database attacker. This Process can be depicted with the below shown algorithm 1. Once the ID is detected for the tampering through the avalanche effect of the hash keys then, the remaining attribute's integrity is being measured through comparing the original data tuples list of the past and current thread of the bilinear pairs, this eventually yields the details of the tampering processes.

Step 4: Tamper Detection And Forensic Analysis- Here in this step the culprit is going to nab using the recursive surveillance on the database log file, Which is in the form of an XML where logs of the database user is traced out by string handling of the XML and correlating his illegal activity with the current and the previous bilinear activities.

Eventually by doing this proposed model successfully got the all the details of database tampering like Who did the Tampering? When did the Tampering? On what attributes tampering was happened?. Once all these parameters are collected, then a proper report is generated to deliver to the admin.

After this process the previous string of the bilinear pair is restored in the database for the tampered ID by updating its all other attributes to get the original database tuples.

Algorithm:

// Input : Database D_B

// Output : Tamperset T_{SET}

Start

PD_{SET} =Ø, CD_{SET} =Ø

[PD_{SET} : Previous DB Set , CD_{SET} : Current DB Set]

PDH_{SET} =Ø, CDH_{SET} =Ø

[PDH_{SET} : Previous DB Hash Set , CDH_{SET} : Current DB Hash Set]

CD_{SET} → getDatabaseList

CDH_{SET}→ Hashset of CD_{SET}

while TRUE

WAIT FOR **T** [Tile: Time]

PD_{SET} → CD_{SET}

PDH_{SET} → CDH_{SET}

for i=0 **to** size of CDH_{SET}

IF CDH_{SET} ≠ PDH_{SET} **THEN**

check CD_{SET} and PD_{SET} for Details

Generate Report $\mathbf{G_R}$

T_{SET} = T_{SET}+$\mathbf{G_R}$

End for

End While

return T_{SET}

Stop

Module Description:

1) Module A: Validator

- Input: Time in minutes
- Process: Recursive Database visiting
- Output: Access Database

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

2) Module B: Bilinear Pairing

- Input: Tile
- Process: Database Tuple Access
- Output: Tuple in between a tile

3) Module C: Avalanche Effect

- Input: Two tuples
- Process: Tuple hash and hash validation.
- Output: Hash Inequality estimation

4) Module D: Temper Detection

- Input: Hash Inequality estimation
- Process: Tuple attributes String
- Output: Tampered ID

5) Module E: Forensic Analysis

- Input: Tampered ID
- Process: Forensic Parameter Evaluation like Who, When and Where
- Output: Report Generation

IV. RESULTS AND DISCUSSION

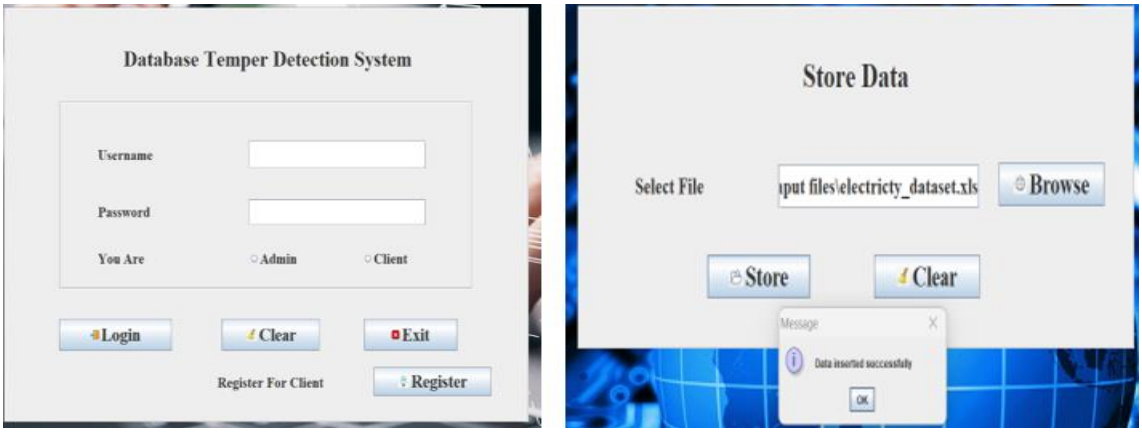

Figure 2: Client Store Data

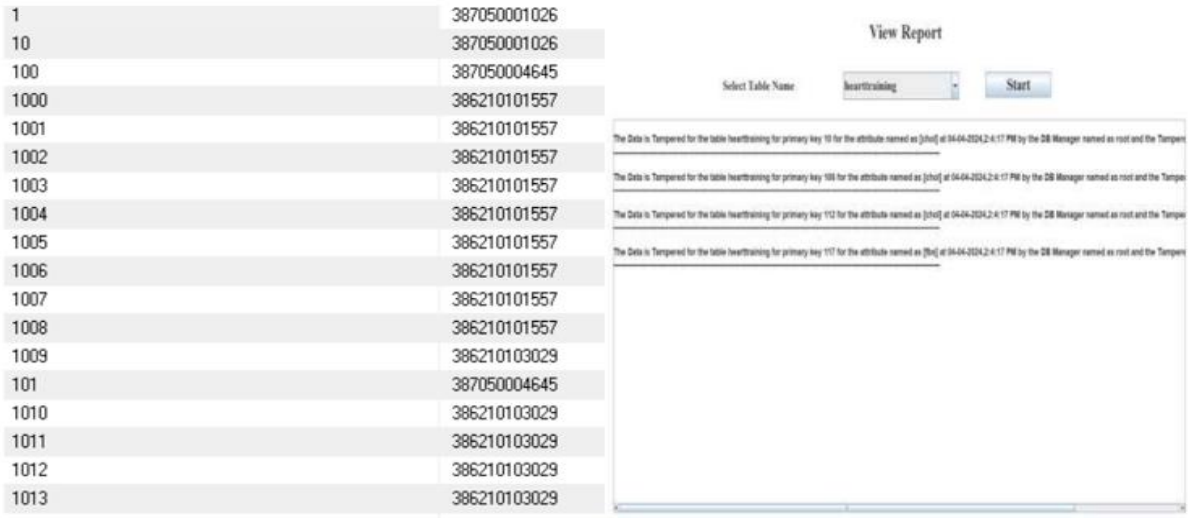

Figure 3: Database Tamper Detect

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

V. CONCLUSION

Due to increasing in outsourcing data storage at warehouse in drastic speed, So threat to the data is also increasing like anything from inside intruders. Our proposed method implements anti data tampering technique using tiled bitmap process which is powered with the avalance effect concept.

On observing the performance of the system it clearly indicates that this process is very effective in handling database tampering and recovering system for huge size of the databases.

VI. REFERENCES

[1] Davenport and S. Shetty, "Air Gapped Wallet Schemes and Private Key Leakage in Permissioned Blockchain Platforms," 2019 IEEE International Conference on Blockchain (Blockchain), 2019, pp. 541-545, doi: 10.1109/Block chain.2019.00004.

[2] K. Rani and C. Sharma, "Tampering Detection of Distributed Databases using Blockchain Technology," 2019 Twelfth International Conference on Con-temporary Computing (IC3), 2019, pp. 1-4, doi: 10. 1109/IC3. 2019. 8844938.

[3] H. Guo, W. Li, M. Nejad and C. Shen, "Access Control for Electronic Health Records with Hybrid Blockchain-Edge Architecture," 2019 IEEE International Conference on Blockchain (Blockchain), 2019, pp. 44-51, doi: 10.1109/Blockchain.2019.00015.

[4] J. Zhang, S. Zhong, J. Wang and L. Wang, "An Systematic Study on Blockchain Transaction Databases Storage and Optimization," 2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), 2020, pp. 298-304, doi: 10.1109/ISPA-BDCloud-SocialCom-SustainCom51426.2020.00 063.

[5] S. Linoy, H. Mahdikhani, S. Ray, R. Lu, N. Stakhanova and A. Ghorbani, "Scalable Privacy-Preserving Query Processing over Ethereum Blockchain,"2019 IEEE International Conference on Blockchain (Blockchain), 2019, pp.398-404, doi: 10.1109/Blockchain.2019.00061.

[6] S. Sahai, M. Atre, S. Sharma, R. Gupta and S. K. Shukla, "Verity: Blockchain Based Framework to Detect Insider Attacks in DBMS," 2020 IEEE In-ternational Conference on Blockchain (Blockchain), 2020, pp. 26-35, doi: 10.1109/Blockchain 50366.2020.00012.

[7] E. S¸afak, A. F. Mendi and T. Erol, "Hybrid Database Design Combination of Blockchain And Central Database," 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 2019,1-5, doi: 10.1109/ISMSIT.2019.8932763.