SSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 6, Issue 9, March 2017

An Advanced Watermark Technique on Relational Database

Alfia Khan, DharaNarodiya, Prof. Mahesh Korade

Abstract*— Growth in the information technology is playing an increasing role in use of informationsystems having relational databases. These relational databases are used very effectively in the computer environments for information extraction. They are exposed to security threats concerned by the ownership rights. Watermarking is used to enforce ownership rights about the shared relational data and for providing a means of tackling data tampering. When ownership rights are applied using watermarking, the underlined data undergoes certain modifications, as a result of which the data quality gets no attention. The reversible watermarking technique is employed to ensure data quality along with the recovery of the database. Such techniques are usually not robust against attacks and do not provide any method to select and apply a watermark on a particular attribute by taking into the picture its part in knowledge discovery. Hence the reversible watermarking is required that ensures the watermark encoding and decoding by accounting for the act of all the features in knowledge discovery. A robust and reversible watermarking (RRW) technique for the numbers relational data has been proposed that corresponds to the above objectives. Researches prove the effectiveness of reversible and robust watermarked technique against malicious attacks and shows that the proposed technique outperforms present ones.

***Index Terms*—Reversible watermarking, Data recovery, Data Quality, Numerical Data, Encoding and Decoding.**

I. INTRODUCTION

In today's digital world, data is increasingly being generated due to the increasing use of the Internet and Cloud Computing. Data is stored in different digital formats such as audio, text, video and relational data. Relational data in particular is shared mostly by the owners with research bodies and in virtual data storage locations on the Cloud. The purpose is to work in effective environment and make data openly available so that it is useful for knowledge extraction. Take the case of Wal-Mart a large multinational retail corporation company that has made its sales database available openly on the Internet so that it can be used for the purposes of identifying market trends and researches. These open available databases make attractive targets for malicious attacks. For example there are documented attack examples where data containing personal logs of the workers and customers using the Wal-Mart services were stolen. According to a survey related to the security of customer data, it is reported that 48% of organizations do notconsider security and privacy problems when sharing their confidential data. Therefore, 62% organizations have to face data loss repeatedly. Similarly, data stealing andcorrupting in the health care and medical domain are increasing. Hence it is imperative that in shared environments such as the cloud, security issues that arise from an un-trusted relational database need to be addressed also with the application of ownership rights on behalf of their owners. Watermarking techniques have been used to security in terms of ownership protection and data security for a wide variety of data formats. This includes texts, images, audios, videos and natural language processing software, relational databases and much more. The robust and reversible watermarking method can make sure of the data recovery along with ownership protection rights. Fingerprinting, data hashing, serial codes are some of the other techniques used for ownership protection. Fingerprints also called transactional watermarks are used to identify and monitor digital ownership by watermarking all the copies of contents with different watermarks for different customers. Firstly this type of digital watermarking tries to identify the source of dataleakage by tracing guilt of the agent. In hashing, digital contents can be saved by performing a one-way hash function whereby the data contents does not change. If the hash of the original and tampered data is the same, data privacy can be verified but ownership cannot be proved very easily. The serial or classified nodes are used for filtering of the contents which is not appropriate over the Internet and are mainly applicable to images, audio and video. Watermarking can provide with the ownership protection over the digital content by marking the data with a watermark which is unique to the owner. After that the embedded watermark can subsequently be used for proving andclaiming ownership of the user.

II. LITERATURE REVIEW

A Method for the Trust Management in Cloud Computing: Data Coloring by using the Cloud Watermarking Technique-In this paper, they have proposed a data coloring method which is based on the cloud watermarking to recognize and ensure mutual reputations. The researched results show that the robustness of reverse cloud generator can guarantee the users embedded social reputation identifications. Hence, the work provides a reference solution to the critical problem of cloud security.Public and Secret Key Image Watermarking Schemes for Image Authentication and Ownership Verification-The scheme can analyze any modification that has been made to the image and indicate that the particular locations that have been modified to the database. If the valid key is specified in the watermark extraction procedure, after that an output image is returned showing a proper watermark, proving

SSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 6, Issue 9, March 2017

the media is authentic and has not been changed since the application of the watermark technique. It needs a user key during both the insertion and the extraction processes, it isn't possible for a user who is not authorized to insert a new watermark or alter the existing watermarks so that the resulting image will pass the test. They present secret key and public key versions of the technique.RRW - A Robust and Reversible Watermarking Technique for Relational Database-Advancement in information technology is playing a very important role in the use of information systems comprising relational databases. These databases are used effectively in computational environments for information extraction; consequently, they are exposed to security threats concerned by the ownership rights and data tampering issues. Watermarking technique is used to enforce ownership rights over shared relational database and to provide a means for tackling data tampering. After the ownership rights are applied using watermarking, the underlined data goes through certain modifications, as a result of which the data quality gets compromised. Reversible watermarking is employed to ensure data quality along-with data recovery. However, such techniques are usually not robust against malicious attacks and do not provide any mechanism to selectively watermark a particular attribute by taking into account its role in knowledge discovery. Therefore, reversible watermarking is required that ensures the data recovery and ownership privacy.

III. MATHEMATICAL MODELING

U=D,P,G,W,O,F,I, Where
I D1, ...Dn Set of input data
P=Pl, ...Pn Set of parses for reading the data
W=Wl, ...Wn Set of generated watermark that has to be embedded
0=G1,.....Gn Set of classfied generated data from input data
0 01, ...0n Set of output data obtained by the watermark

F=, ...fn Set of functions used to recover watermark1=I1, ...In Set of data that is generated after recovery of the watermark.

Functions:-

f1(D) 1-, P : Function that passes the input data to parser
f2(D,P) '-' G : Function that parses the data and generates G

f3 (G) i- W : Function that generates watermark data fa(D,w)

IV. IMPLEMENTATION

For the implementation of Data Tracing Lineage Framework, we have implemented database explore, watermark creation, watermark extraction, compare database, and find database attack percentage using data changes (insert/update/delete) in the database. We used our own database files for the training and testing of our framework.

A. Watermark creation

It select the original database and extract data from the database, Create watermark data using specified columns and number of bits, and Save watermarked database.We select the database by browsing the database file which we want to watermark . There are number of coloums in database such as id, ename, city, age which can be also called as features of that database . After this we select the feature name or column in which we want to make watermark by changing there bits in columns. After this the watermark database has been created. Then save the watermark database.

B. Watermark extraction

Select watermarked database and Extract original data using specified columns and number of bits, Save original data.In this we select the databse file which is been watermarked by the owner. Select the same feature which we have selected in the creation process to check weather the attacker have made any changes in the original watermark. Then it saves the extracted file in the database.

C. Compare original database and watermarked database

Selects the original file in which it select the table by browsing the database file. Then we selects the extracted database file which also contain the table to be selected by browsing the database. Then it compares the original data with the extracted data. By which we come to know the percent of attack done on the original database. It also shows the attack done in which column and rows.

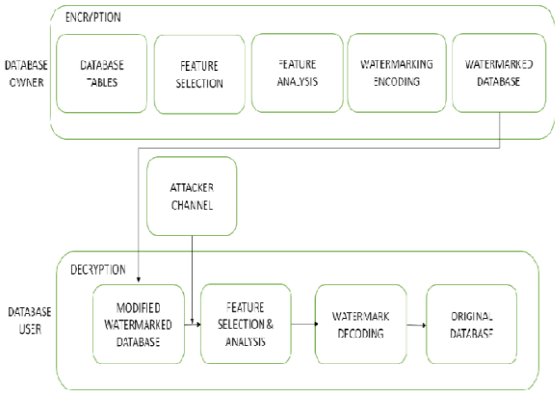
D. Objectives

The main goals of using watermarking technique is used to ensure security in terms of ownership protection in the multimedia data. To apply it on relational data to maintain the security and ownership of the data.

E. Applications

- Business
- Colleges
- University

F. Architecture



SSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 6, Issue 9, March 2017

V. CONCLUSION

Irreversible watermarking techniques make changes in the data to such an extent that data quality gets compromised. Reversible watermarking techniques are used to cater to such scenarios because they are able to recover original data from watermarked data and ensure data quality to some extent. However, these techniques are not robust against malicious attacks particularly those techniques that target some selected tuples for watermarking. In this paper, a novel robust and reversible technique for watermarking numerical data of relational databases is presented. The main contribution of this work is that it allows recovery of a large portion of the data even after being subjected to malicious attacks. RRW is also evaluated through attack analysis where the watermark is detected with maximum decoding accuracy in different scenarios. A number of experiments have been conducted with different number of tuples attacked. The results of the experimental study show that, even if an intruder deletes, adds or alters up to 50of tuples, RRW is able to recover both the embedded watermark and the original data. RRW is compared with recently proposed state of the art techniques such as DEW, GADEW and PEEW to demonstrate that RRW outperforms all of them on different performance merits. One of our future concerns is to watermark shared databases in distributed environments where different members share their data in various proportions.We also plan to extend RRW for non-numeric data stores.

ACKNOWLEDGEMENT

It gives us great pleasure in presenting the paper on 'An AdvancedWatermarking technique on relational database'. I would like to take this opportunity to thank my internal guide Prof. Mahesh Koradefor giving me all the help and guidance I needed. I am really grateful to them for their kind support. Their valuable suggestions were very helpful. I am also grateful to Prof. K.C.Nalavade, for his indispensable support, suggestions. In the end our special thanks to Prof. Amit G. Patil for providing various resources such as laboratory with all needed software platforms, continuous Internet connection, for Our Project.

REFERENCES

[1] Y.-C. Liu, Y.-T. Ma, H.-S. Zhang, D.-Y. Li, and G.-S. Chen, "A method for trust management in cloud computing: Data coloring by cloud watermarking," International Journal of Automation and Computing, vol. 8, no. 3, pp. 280– 285, 2011.

[2] Walmart to start sharing its sales data," http://www.nypost.com/p/news/business/walmart-opensup, last updated: 09:55 AM on February 4, 2012, last accessed: July, 20 2013.

[3] "Identity theft watch," http://www.scambook.com/blog/2013/ 04/identity-theft-watch-customer-passwords-stolen-fromwalmart-vudu-video-service/, last updated: April 11, 2013, last accessed: July, 20 2013.

[4] "Securing outsourced consumer data," http://www.databreaches.net/securing-outsourced-consumerdata/, last updated: February 26, 2013, last accessed: July, 20 2013.

[5] "As patients' records go digital, theft and hacking problems grow," http://www.kaiserhealthnews.org/Stories/2012/June/04/ electronic-health-records-theft-hacking.aspx, last updated: June 03, 2012, last accessed: July, 20 2013.

[6] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," Image Processing, IEEE

[7] Transactions on, vol. 6, no. 12, pp. 1673–1687, 1997.

[8] I. Cox, M. Miller, J. Bloom, and M. Miller, Digital watermarking. Morgan Kaufmann, 2001.

AUTHOR BIOGRAPHY

Alfia Khan

I have completed my schooling from boys town public school. I did my diploma from jmctpolytechniquenashik. Currently I am persuing my degree from Sandip Institute of Engneering and Management (SIEM) Nasik.

Dhara Narodiya

I have completed my schooling from St Lawerence High school. I did my diploma from Guru Gobind Sigh polytechniqueNashik. Currently I am persuing my degree fromSandip Institute of Engineering and Management (SIEM) Nashik.

Mahesh.V.Korade

Asst. Professor Sandip Institute of Engineering and Management His area of interest is S/W Engg., Operationsyst, Networking.