

Watermarking Technique using UID for Relational Data Saving in Database

G. Agila
Research scholar,
Dept of CSA, SCSVMV University

N.R. Ananthanarayanan, PhD
M.C.A.,M.B.A.,I.D.C.P.A.,Ph.D
Associate professor,
Dept of CSA, SCSVMV University

ABSTRACT

The technology is increasing to use the information in relational data for saving in database. This database are used in collaboration of environment is used to exact the data and the data is need to security threat for ownership rights. The watermarking is enforcing the data saving the ownership rights in relational data saving in database. In this watermarking technique was containing both reversible and non reversible technique for data storage and recovery. The watermarking technique was providing security threats concerning the ownership rights. The attacking the data saved in database which was in EyeOs cloud server to solve this problem in this watermarking technique using UID for relational data saving in database using four steps modules for encoding and decoding the discovery knowledge (data). Watermarking technique contains the following steps. They are step one is to encoding and decoding the data saved in database step two is to discover of the knowledge of original data saved in database protected from attacker.

Keywords

UID, Unique Identification, CS, Checksum CT, Cyber text, DES, Data Encryption Standard TS, Time Stamp RCS, Row Checksum BC, Binary conversion .

1. INTRODUCTION

Main purpose of project

The main aim of this project is the watermarking technique using UID (Unique Identification) for relational data saving in database is to maintain ownership of relational data saved in the database and also to minimizing distortion in the content in watermarked data is saved in database.

Project Scope

The main of this project is to Watermarking method is to recognizable pattern used to identify authenticity This watermarking technique using UID(unique Identification) for relational data saving in database is to identify authentication user or attacker of data and used for ownership protection number of data. The data stored in cloud storage that is EyeOs cloud. It was virtually stored free web based operating system (OS). This EyeoOs is available in both cloud that is private cloud and public cloud. It was used for file management, user management similar take our desktop in computer Personal Computer (PC).the user can preserve the knowledge contained in the data and data can save in EyeOS System Structure is divided in three components such as Client, Web Server, and Database Server to store data in database. The purpose of this project is to work in the collaborative environment and this was make data was openly available for the user to find the knowledge to discover and also to the extraction of knowledge this project is useful for decision making to save the data from the attacker or hacker of data.

Overall Description

This proposed system of the project was implementing a new idea for the data to generate the watermark bits UID (Unique Identify). Which was using the checksum that was used as the keyword this was based on the data time.In the database while saving the data was used effectively in collaboration of saving in environments for information extraction of data? It just wants to hide the data in the database. In this project while the verhoeff algorithm is to generate the checksum for the data by using this checksum randomly selected the rows and columns we can hide or watermark the data. Encoding phase consist of Data partitioning, Selection of data set for watermarking, Watermark embedding process saving the data and Decoding phase consist also these process to extract the Watermarked content saving the data. EyeOS System Structure is divided in three components such as Client, Web Server, and Database Server to store data in database.

This project of saving the data in vulnerable to security for the threats was attack ownership rights and this unique identify (UID) was also saving the data tempering which was openly available the data is to set as target for the attacking person or hacker of the data. To overcome this problem in this project as to apply the watermarking concept in the numerical that is number was used as data which was saving in database. This is the different way for saving the data in database and also we can achieve the data for safety recovery from database in EyeOs cloud server.

2. EXISTING SYSTEM

This existing system which is describes the points taken for reference for this project for saving data in database. These points taken for existing project using the watermarking technique.

- From the [1] reference book main point is a bit resetting algorithm is to employs for the principle of the setting the data that data is selecting least significant bit that is [LSB] of the candidate that set of rows and columns attribute of the selected subsets of tuples.
- From the [2] reference book point is reversible watermarking is employed is to ensure the data that is rows and columns the ensure the data quality along with data recovery.
- From the [3] reference book such type of techniques is to usually not robust against malicious attacks of data in database and do not provide any mechanism to selectively watermark data is contain the database which particular the attributes in rows and columns which was taking the account the knowledge discovery.

- From the [4] reference book although LSB based data hiding techniques are host efficiency for the saving data in database but the attacker or hacker is to able to easily remove the watermarking technique by simply using the manipulation of data by shifting technique.
- From the [5] reference book the data was partitioning concept is based is to used for the special maker that is the data was selected as tuples and making the vulnerable to watermark for the synchronization of the errors was occurred in the data saving in the database.

3. PROPOSED SYSTEM

In the proposed system of the Watermarking Technique using UID for Relational Data Saving in Database we as newly implement as new approach to generate the watermark bit by using UID (Unique Identification) bit. In this project watermarking concept is contain the numerical database (that is data was numbers) in the different way of using the MSB (Most Significant Bit). This technique was checking the data by right to left by using this type and we have use verhoeff algorithm this algorithm was generate the checksum value. The checksum value means the count the number of bits in a transmission of unit of data that is receiver can check the same number of bit while arriving of data if the count of data that is checksum value was must completely mach the transmission of receiving the data. In this project verhoeff algorithm was used verhoeff algorithm is used for checksum value using the check sum value formula is used for error detect of data in database. This verhoeff was finding the decimal code that is checksum value by using single decimal digit.

From the single decimal digit checking by MSB (Most Significant Bit) is also called the high order bit the bit was check from right single decimal digit to left single decimal digit. Then the value of embedding the watermark that current time stamp. The time stamp is encoded Information was event occurred by using the date and time of the current day of saving the information.

That value of information is taken into key value by using the key value hash function was used to find cyber text value. The hash function is used to make the map of data to fix the size or value. That value return by the hash function is called the hash values that values match only the key values. The Watermarking process includes the values of Encoding and Decoding Phase using the UID (unique identification) Then the authentication channel have two types of authentication system first step the enter the user name and user phone number then second step user got the OTP that is one time password by sms then server validate the OTP it generate the randomized virtual keyboard pattern then the server can send to user mobile using SSL (Secure Socket Layer) protocol via sms provider.

After generating all value decode the full values of data in the database then user can discover the original values. The Encoding phase consist of Data partitioning, Selection of data set for watermarking, Watermark embedding process .Decoding phase consist also these process to extract the Watermarked content saving the data in database on EyeOs cloud. The figure from the main of architecture diagram given below Watermarking Technique using UID for Relational Data Saving in Database

4. MODULES OF UID TECHNIQUE

There are four types of modules in watermarking technique using UID for relational data saving in database. The modules are given below

- Generate numerical data and check sum values.
- Watermark embedding in database using UID.
- User authentication channel to proof the ownership.
- Identify checksum and recover the data.

5. GENERATE NUMERICAL DATA AND CHECKSUM VALIDATION

In this project we choose the numerical database for embedding watermark because the attacker or hacker is hard to find out the watermark data in database was saved by owner is hard to compare to alpha numerical dataset. In the numerical data set the data was contain the only numeric data for each rows and columns for example patient of all record was maintained by the numerical data and it was based on the high security issues so now we can take only the numerical data set then the data each records in the database are must contain the unique identification.

Validate checksum using verhoeff algorithm

Input UID

Output B

For i=1to UID Length do

//loop will iterate for all numeric data in database

c= d[c][p[((i + 1) % 8)] [UID [i]]];

End for

Return (c == 0)

UID=Unique identification for data

Cs=Checksum for data

d= // the multiplication table in rows and column

p= // the permutation table in rows and column

c=//Number variable for data

To Generate The Check Sum Value

First thing is to generate the check sum values is a collect the data in numerical form then the data set is contains in rows and column each and every rows as a person/patient information so now we select one unique identification column. That unique identification column for all rows to generate the checksum value for person/patient. That unique identification column takes as input for the starting point of watermark embedding process then we used the verhoeff algorithm. This verhoeff algorithm is to generate the check sum value (Verhoeff algorithm check sum formula for error detection).

To validate a checksum using verhoeff algorithm this verhoeff algorithm is check sum formula for error detection data which was saved in database and this formula was strength of the algorithm are that it detects all transliteration of data in database and transposition of error in data which was saved in database.

6. WATERMARK EMBEDDING IN DATABASE USING UID

The watermark embedding technique is mostly used LSB Technique (Least Significant Bit) that data was check from left bit to right bit this technique is easy for attacker or hacker can find the watermark content using the shift operation to solve this problem in this project we used the MSB technique (Most Significant Bit) this step for more security issues.

Formula for Binary Number Converts InTo Numerical Data

$Ct=DES ((R.Cs) TS)$ -----Equation 1 for convert value to cyber text

$BN=BC (Ct)$ -----Equation 2 for convert value to binary number

R.Cs=Row checksum for data

Ct=Cyber text for data

DES=(DES)Algorithm for data

TS=Timestamp for data

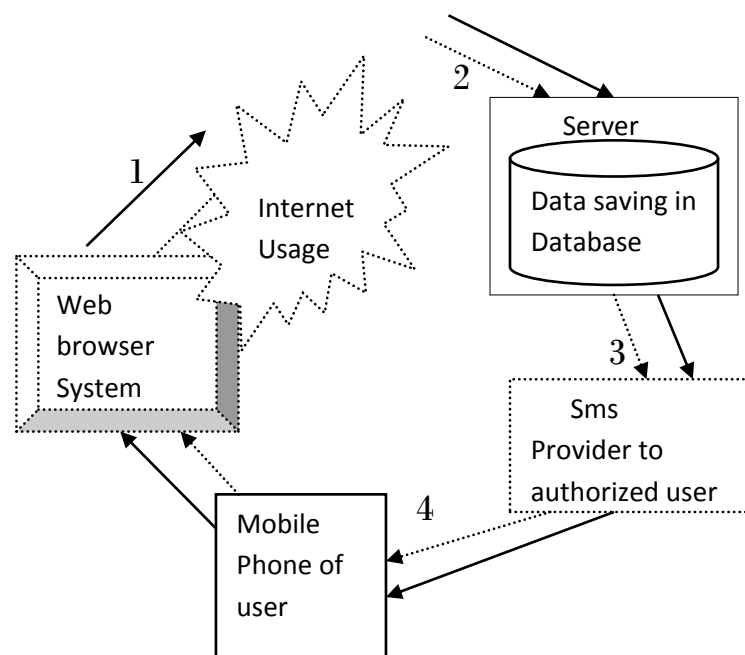
BC=Binary conversion for data

Embedding Watermark The Data

When the data owner was embedding the watermark the data in database that was current time stamp that is current date and time of current data saving then the time stamp was been taken the key for the data saving. That key value is check sum for validated the hash value (Cyber Text). Hash function is used for map the data where it was fixed by using the hash value that is cyber text value is assign the Data Encryption Standard (DES) algorithm. The Data Encryption Standard (DES) algorithm is symmetric key of algorithm for encryption of data. In proposed system fixed length of data that is string of plain text bit of data was transform when one operation as performed into another cyber text bit string of same length it was used only in encrypt and decrypt of same bit.

In the project DES algorithm was using time stamp has to share secretly of data transmission then the cyber text was convert into binary number using binary conversion algorithm. When the binary conversion algorithm process the numerical data into 0's and 1's bit. Then the numerical row values is convert into binary number for embedding the secret key then the binary number is insert into corresponding row using MSB technique (Most Significant Bit). Then the process has been performed after embedding the secret key binary number is converting into numerical data

User Authentication Channel Architecture Diagram



From the above figure User Authentication Channel Architecture Diagram explanation are given below

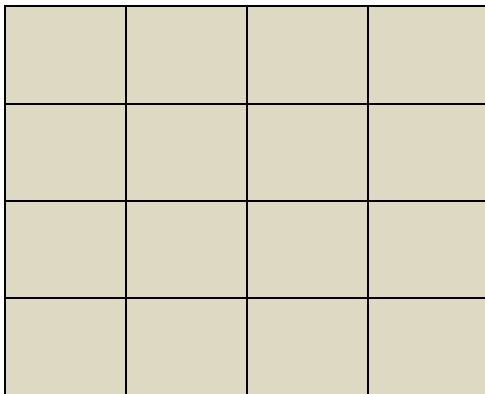
- [1] To check the Authorized user using web browser via internet the system show that user. Then enter the user name and user phone number.
- [2] After user enter detail of user name and password system send information to the server. The server check authorized user or data hacker from database.
- [3] Check the detail from database server sends the sms provider from http protocol. This technique is for unauthorized person does not decode watermark.
- [4] From sms provider receive message from server which was analyzed from database. After receive the message from mobile and User can check message and enter the secret message to decode watermark technique.

7. USER AUTHENTICATION CHANNEL TO PROOF THE OWNERSHIP

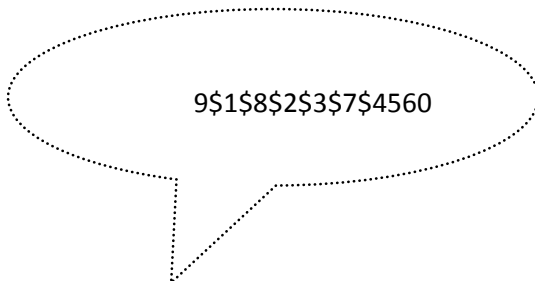
When watermark embedding in database using UID encoding the data by using the time stamp then user to identify the ownership of data. In this project user authentication channel have two authentication systems. A user first gets the credential to authenticate the system then user enters the username and user phone number for user identification of user or attacker found. This method is for security issues. While the user enter the data then server check user request then the server via http protocol, check the user credential verify the authentication user or not. Then the server send the OTP (One Time Password) to user mobile number via sms provider then the user again enter the OTP and send the server. Once again server can entered data by using randomized virtual keyboard pattern and server again send to user by mobile using SSL (Secure Socket Layer) protocol via sms provider. SSL (Secure Socket Layer) is standard security technology for establishing an encrypted the link in data

between a server and user by using the website, web browser, mail to server, mail to client.

Eg: Random virtual keyboard in web browser used only authorized user



SMS Decrypted pattern in mobile phone for check authorized user:



When the random virtual keyboard pattern is encrypted using RSA algorithm. The RSA algorithm is modern computer was using the encryption and decryption of the message saving or data saving in database. In this proposed system asymmetric crypto graphical algorithm by using two different keys. One key was using private and other key was private key. In this project RSA algorithm was send to user mobile via sms provider and decrypted the random virtual keyboard pattern in user mobile when the user can click the password in browser using based on the randomize virtual keyboard pattern. Once the user can click his password then the index is to send for server once the server can identify the index and validate the user index based on the password then the user can send then the password once the validation is success then the user is authorized user or then the user is unauthorized user that is hacker or attacker of the data in the database.

8. IDENTIFY CHECK SUM AND RECOVER THE DATA

After finishing the user authentication channel to proof the ownership now owner can access the data that is decode all the process. Again first step of module one verhoeff algorithm was again process for decode the data in database. When the

user wants to access the data after successful authentication another credential is there for access the data in database.

Algorithm 2 Validate Checksum For Data Recovery:

Input UI

Output B

For i=1 to UI Length do

//loop will iterate for all numeric data in database

c= d[c][p[((i + 1) % 8) [UI [i]]];

End for

Return (c == 0)

Data Recovery

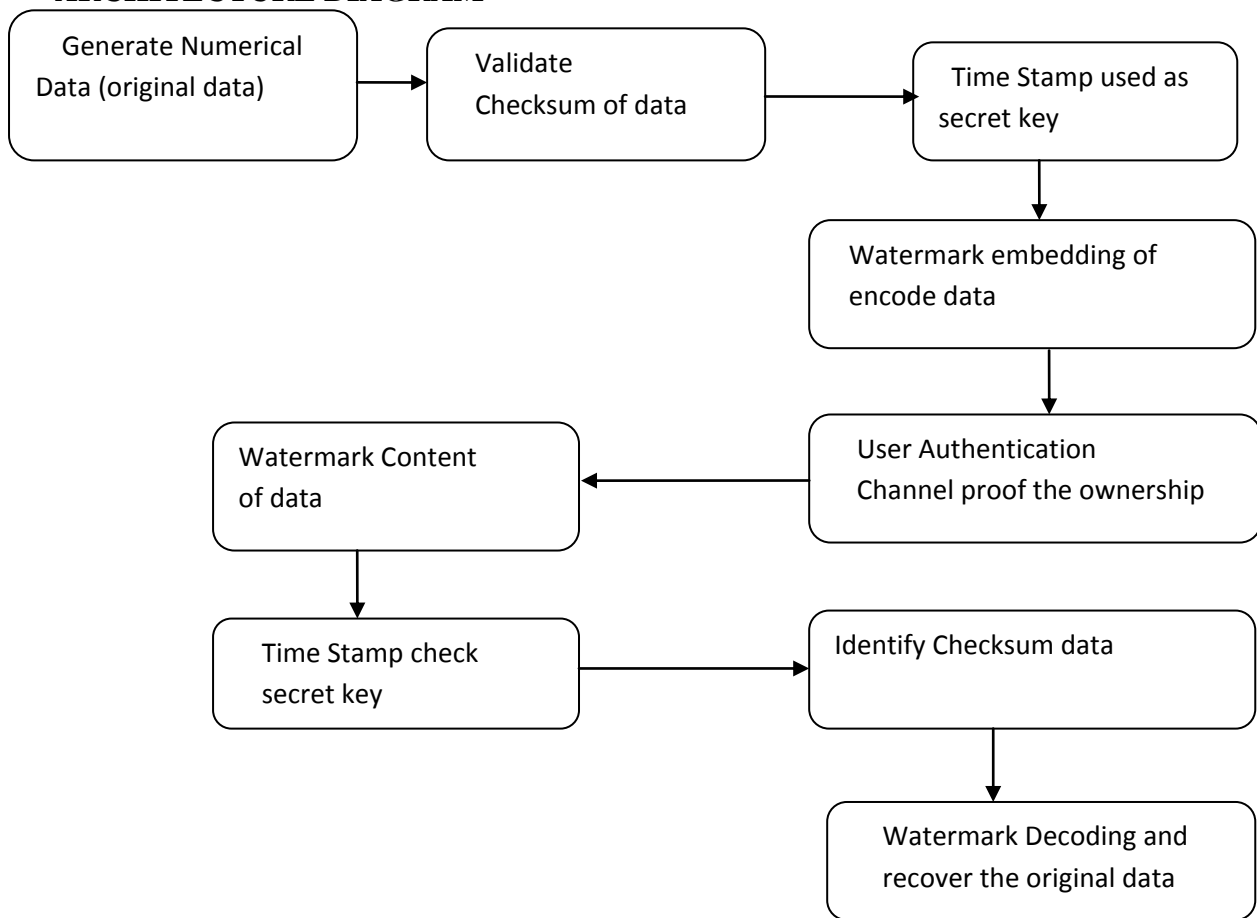
When the user can enter the time stamp that is date and time to the server to the server can extract the numerical data set in data base. When the data was convert into binary value. Then the binary value be get to inserted secret key values when the secret key for binary digit for MSB (Most Significant Bit) values in corresponding rows as been check from right side to left side.

Then the data was convert the MSB secret key binary digit into the cyber text value here cyber text value is hash function value that can fix only by the fixed size of data. When the cyber text value is decrypted using the DES (Data Encryption Standard) algorithm using time stamp. After the decrypted value is checked whether that the value is valid checksum for that the corresponding person or hacker of the data. If the check sum is valid the data will be data saved in the database was recovered that knowledge was discovered otherwise the data is not recovered and server was identify the user was attacker.

9. USER CLASSES AND CHARACTERISTICS

- Fetch.java is used for to summarize the fetch records..
- Datapartition.java is used for to summarize the data partition records.
- Tupleselection .java is used for to summarize the tupleselection records.
- Embedding .java is used for to summarize the embedding records.
- decoding .java is used for to decoding record

10. WATER MARKING TECHNIQUE USING UID FOR RELATIONAL DATA SAVING IN DATABASE ARCHITECTURE DIAGRAM



11. SYSTEM REQUIREMENTS SOFTWARE REQUIREMENTS

- Windows operating system XP
- JDK 1.6
- Mysql 6.0
- Oracle 10g

12. HARDWARE REQUIREMENTS

- Hard Disk : 40GB and Above
- RAM : 512MB and Above
- Processor : Pentium IV and Above

13. DESIGN AND IMPLEMENTATION CONSTRAINTS

13.1 Constraints in Analysis

- Constraints analysis as Informal Text
- Constraints analysis as Operational Restrictions
- Constraints analysis as Integrated in Existing Model Concepts

- Constraints analysis as a Separate Concept

- Constraints analysis as Implied by the Model Structure

13.2 Constraints in Design

- Constraints in design is to determination of the Involved Classes
- Constraints in design is to determination of the Involved Objects
- Constraints in design is to determination of the Involved Actions
- Constraints in design is to determination of the Require Clauses
- Constraints in design is to Global actions and Constraint Realization

14. CONSTRAINTS IN IMPLEMENTATION

A hierarchical structuring of relations may result in more classes and a more complicated of data structure to implement saving data in the database. In this project is too advisable to transform the hierarchical relation structure to a simpler to the

same structure. It is rather straightforward to transform data to developed hierarchical model into a flat model, consisting of classes on the one hand and flat relations on the other while saving data in database. Flat relations are preferred at the design level for reasons of simplicity and implementation easy in saving data in the database. There is no identity or functionality associated with a flat relation between data saving in database. A flat relation corresponds with the relation concept of entity-relationship modeling and many object oriented methods of saving data in database.

14.1 System Features of UID

In this present a new routing algorithm in which a node forwards its messages that is data the nodes that contain the destination node in their ownership communities. To reflect the periodic changes on node relations, in this project the ownership communities depend on the period of day in which forwarding is done that this timestamp. So it can make easy for the owner save the data day by day in database.

15. EXTERNAL INTERFACE REQUIREMENTS OF UID USER INTERFACES

1. All the contents are used in the project are implemented using Graphical User Interface (GUI) of JavaFX.
2. Every conceptual part of these projects is used to reflect using the FX.
3. In this project the System gets the input and delivers through the GUI based.

15.1 Hardware Interfaces of UID:

Ethernet

Ethernet on the AS/400 supports TCP/IP, Advanced Peer-to-Peer Networking (APPN), advanced program-to-program communications (APPC) and sever socket layer (SSL).

ISDN

In proposed system user can connect your AS/400 to an Integrated Services Digital Network (ISDN) for faster, more accurate data transmission of data saving in database. An ISDN is a public or private digital communications network that can support data, fax, image, and other services over the same physical interface with system. Also, you can use other protocols on ISDN, such as IDLC and X.25 access server.

15.2. Software Interfaces of UID:

In this project we used software is too interacted with the Http protocol. This protocol is running in tomcat port number (default 80).

15.3 Communications Interfaces

- 1 TCP/IP protocol.
2. SSL protocol.
3. LAN Settings.
4. Http protocol

15.4 Other Nonfunctional Requirements of UID

Performance Requirements of UID:

In is proposed system user can need to one or more than one machine to execute the demo? Machine needs the enough hard disk space to install the software to run this project. The

entire machine should be connected with LAN settings. Thereafter we have to do the basic configurations settings and its useful for saving cloud EYEOS.

16. SAFETY REQUIREMENT OF UID

1. In this project safety requirement is the software may be safety-critical. If so, there are issues associated with its integrity level.
2. In this project safety requirement is software may not be safety-critical although it forms part of a safety-critical system. For example, software may simply log transactions.
3. In this project safety requirement is if a system must be of a high integrity level and if the software is shown to be of that integrity level, then the hardware must be at least of the same integrity level.
4. In this project safety requirement is there is little point in producing 'perfect' code in some language if hardware and system software (in widest sense) are not reliable.
5. In this project safety requirement is if a computer system is to run software of a high integrity level then that system should not at the same time accommodate software of a lower integrity level.
6. In this project safety requirement is systems with different requirements for safety levels must be separated.
7. In this project safety requirement is otherwise, the highest level of integrity required must be applied to all systems in the same environment.

16.1 Security Requirements of UID

Do not block the some available ports through the windows firewall.

Software Quality Attributes of UID

- **Functionality:** In this project functionality is required functions available, including interoperability and security.
- **Reliability:** In this project reliability is maturity, fault tolerance and recoverability
- **Usability:** This project usability is how easy it is to understand, learn, and operate the software system
- **Efficiency:** This project efficiency is performance and resource behavior.
- **Maintainability:** This project maintainability is maintaining the software.
- **Portability:** This project portability is can the software easily be transferred to another environment, including install ability

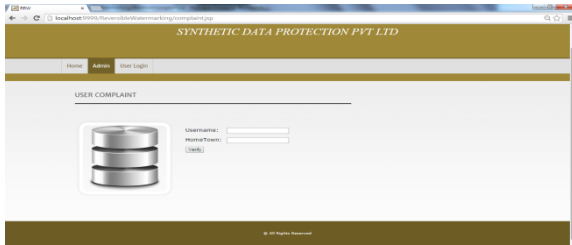
17. APPENDIX A: GLOSSARY

- IU - Unique Identification
- MSB -Most Significant Bit
- DES -Data Encryption Standard
- OTP -One Time Password

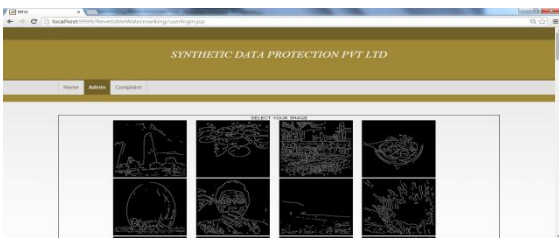
- SSL -Secure Socket Layer
- LAN - Local Area Network.
- TCP/IP - Transport Control Protocol

18. SCREEN SHOTS

Water Marking Technique Using UID For Relational Data Saving:Page1.1:



Water Marking Technique Using UID For Relational Data Saving:page1.2:



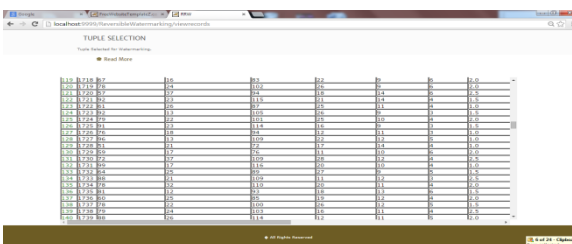
Water Marking Technique Using UID For Relational Data Saving:page1.3:



Water Marking Technique Using UID For Relational Data Saving: page1.4:



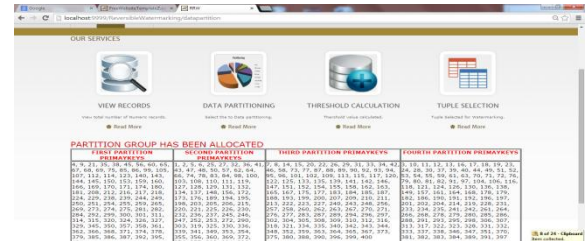
Water Marking Technique Using UID For RelationalDataSaving:page1.5:



Water Marking Technique Using UID For Relational Data Saving: page1.6:



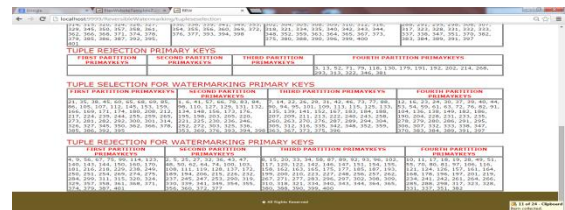
Water Marking Technique Using UID For Relational Data Saving:: page1.7:



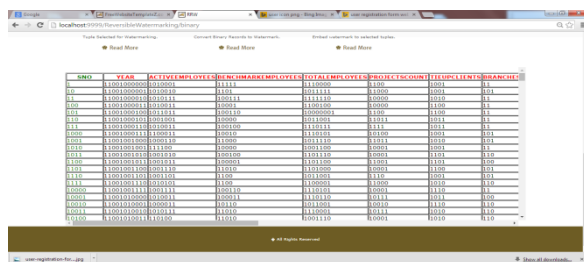
Water Marking Technique Using UID For Relational Data Saving:page1.8:



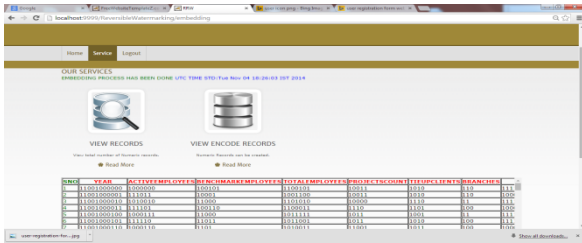
Water Marking Technique Using UID For Relational Data Saving:page1.9:



Water Marking Technique Using UID For Relational Data Saving:page1.10:

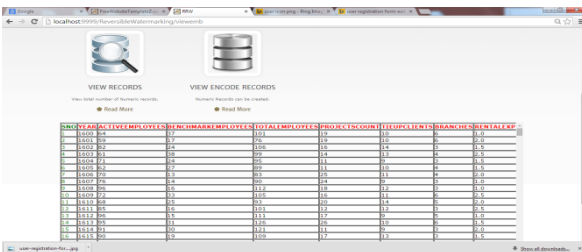


Water Marking Technique Using UID For Relational Data Saving:page1.11:



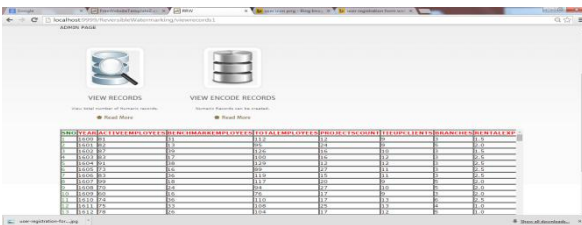
ID	NAME	...
11001000001	11001000001	...
11001000002	11001000002	...
11001000003	11001000003	...
11001000004	11001000004	...
11001000005	11001000005	...
11001000006	11001000006	...
11001000007	11001000007	...
11001000008	11001000008	...
11001000009	11001000009	...
11001000010	11001000010	...

Water Marking Technique Using UID For Relational Data Saving:page1.3:



ID	NAME	...
11001000001	11001000001	...
11001000002	11001000002	...
11001000003	11001000003	...
11001000004	11001000004	...
11001000005	11001000005	...
11001000006	11001000006	...
11001000007	11001000007	...
11001000008	11001000008	...
11001000009	11001000009	...
11001000010	11001000010	...

Water Marking Technique Using UID For Relational Data Saving:page1.14:



ID	NAME	...
11001000001	11001000001	...
11001000002	11001000002	...
11001000003	11001000003	...
11001000004	11001000004	...
11001000005	11001000005	...
11001000006	11001000006	...
11001000007	11001000007	...
11001000008	11001000008	...
11001000009	11001000009	...
11001000010	11001000010	...

19. FUTURE WORK

In future work concerns are to embedding watermark shared data in databases is to distributed environments. Where different members may be shared their data in various proportions. Future work is to plan to extend RRW for non-numeric data stores in cloud platform.

20. CONCLUSION

Watermarking techniques are used to cater to such scenarios because they are able to recover discover the knowledge from watermarked data and this project is ensuring the data quality to some extent. However, these techniques are not robust against malicious attacks – Although MSB-based data hiding techniques are efficient, but an attacker is able to easily to remove watermark or steel the original data by simple manipulation of data by shifting MSB this technique is used for security issues. In this paper, a novel watermark technique using UID. Numerical data of relational databases is presented to EyeOS work as server. This project the server system is structure is divided in three components such as client, web server, and database server to store data in database. The main contribution of this work is that it allows recovery of a large portion of the data saving in database even after being subjected to malicious attacks.

21. REFERENCES

[1] P. W. Wong, “A public key watermark for image verification and authentication,” in Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on, vol. 1. IEEE, 1998, pp. 455–459.

[2] P. W. Wong and N. Memon, “Secret and public key image watermarking schemes for image authentication and ownership verification,” Image Processing, IEEE Transactions on, vol. 10, no. 10, pp. 1593–1601, 2001.

[3] F. A. Petitcolas, “Watermarking schemes evaluation,” Signal Processing Magazine, IEEE, vol. 17, no. 5, pp. 58–64, 2000.

[4] J. T. Brassil, S. Low, and N. F. Maxemchuk, “Copyright protection for the electronic distribution of text documents,” Proceedings of the IEEE, vol. 87, no. 7, pp. 1181–1196, 1999.

[5] R. Agrawal and J. Kiernan, “Watermarking relational databases,” in Proceedings of the 28th international conference on Very Large Data Bases. VLDB Endowment, 2002, pp. 155–166.

[6] CBS News: “Digital piracy stronger than ever”, Online link: <http://goo.gl/Ws2rZ>, valid as of October 2010

[7] Tirkel A., Rankin G., Schyndel R., Ho W., Mee N., and Osborne C.: “Electronic watermark”. Proceedings of Digital Image Computing, Technology and Applications, DICTA 93, pp. 666-673, 1993.

[8] Langelaar G.C., Setyawan I., and Lagendijk R.L.: “Watermarking digital image and video data: a state-of-the-art overview”. IEEE Signal Processing Magazine, Vol.17, pp.20-46, 2000.

[9] Armbrust M, Fox A, Griffith R, Joseph A (2009) Above the Clouds: A Berkeley View of Cloud Computing, Technical Report UCBERECS200928 53(UCB/EECS-2009-28). EECS Department University of California Berkeley

[10] 2. Smith M, Schmidt M, Fallenbeck N, D’ornemann T, Schridde C, Freisleben B (2009) Secure On-demand Grid Computing. J Future Generation Comput Syst 25(3): 315–325

[11] Garfinkel T, Rosenblum M (2005) When Virtual is Harder than Real: Security Challenges in Virtual Machine Based Computing. In 10th Workshop on Hot Topics in Operating Systems 121–126

[12] Reimer D, Thomas A, Ammons G, Mummert T, Alpern B, Bala V (2008) Opening Black Boxes: Using Semantic Information to Combat Virtual Machine Image Sprawl. In Proceedings of the Fourth ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments 111–120. Seattle: ACM

[13] Schwarzkopf R, Schmidt M, Fallenbeck N, Freisleben B (2009) Multi-Layered Virtual Machines for Security Updates in Grid Environments.

[14] In Proceedings of 35th Euromicro Conference on Internet Technologies, Quality of Service and Applications (ITQSA) 563–570. Patras: IEEE Press

[15] Wei J, Zhang X, Ammons G, Bala V, Ning P (2009) Managing Security of Virtual Machine Images in a Cloud Environment. In Proceedings of the 2009 ACM Workshop on Cloud Computing Security, CCSW ’09 91–96. New York: ACM

[16] Fallenbeck N, Schmidt M, Schwarzkopf R, Freisleben B (2010) Inter-Site Virtual Machine Image Transfer in Grids and Clouds. In Proceedings of the 2nd International ICST Conference on Cloud Computing (CloudComp 2010) 1–19. Barcelona: Springer, LNICTS

- [17] Lillard TV, Garrison CP, Schiller CA, Steele J (2010) The Future of Cloud Computing. In *Digital Forensics for Network, Internet, and Cloud Computing* 319–339. Boston: Syngress
- [18] Potter S, Nieh J (2005) AutoPod: Unscheduled System Updates with Zero Data Loss. In *Autonomic Computing, International Conference on* 367–368
- [19] Sapuntzakis C, Brumley D, Chandra R, Zeldovich N, Chow J, Lam MS, Rosenblum M (2003) Virtual Appliances for Deploying and Maintaining Software. In *Proceedings of the 17th USENIX Conference on System Administration* 181–194. Berkeley: USENIX Association
- [20] Debian Security Advisory 1576-1 OpenSSH (2008) Predictable Random Number Generator. <http://www.debian.org/security/2008/dsa-1576>
- [21] Bleikertz S, Schunter M, Probst CW, Pendarakis D, Eriksson K (2010) Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds. In *Proceedings of the 2010 ACM Workshop on Cloud Computing Security, CCSW '10* 93–102. Chicago
- [22] Yoon J, Sim W (2007) Implementation of the, Automated Network Vulnerability Assessment Framework. In *Proceedings of the 4th International Conference on Innovations in Information Technology* 153–157. Dubai: IEEE