International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 09 | Sep-2016 www.irjet.net p-ISSN: 2395-0072

Improvised Security for EAV data model using Negative Shuffled database

Miss Pooja Pandurang Varatk[1], Prof. Amarja Adgaonkar[2], Prof. Neha Jain[3]

[1]*Student, Computer Engineering Department, Shree L.R.Tiwari College of Engineering, Mumbai, India*
[2]*Asst.Professor, Computer Engineering Department, K.C.College of Engineering, Thane, India*
[3]*Assistant Professor, Computer Engineering Department, Shree.L.R.Tiwari College of Engineering, Mumbai, India*

Abstract - *This Paper Presents an improvised security mechanism for EAV (Entity Attribute Value) data model.EAV data model for data storage has been used in various information systems now days as it gives an advantage of data flexibility and addition and modification of new data without changing the physical database schema. In EAV (Entity Attribute Value) model can used in which all data can be stored in single generic table with three columns 1 for entity, 1 for attribute and 1 for value. As data security and database flexibility is important in this paper we are proposing security mechanism for existing databases using concept of negative database and shuffling.*

Key Words: EAV Model, Negative Database, Information Security, Shuffling

1. INTRODUCTION

In our everyday life to store the data database is used in all the fields such as banks, hospitals, colleges, schools etc. If relational database is used to store the data then Physical design of database will get changed, whenever new data types are bring in or existing types are modified.

Also these data need to keep secure from hackers. Hackers try to get access to the private information, which needs to be highly secured. There are several organizations like banks, security agencies, electronic health records, and intelligence applications that need their data to be secured to the highest extent. Various security techniques such as hashing algorithms, encryption algorithms have already been implemented for these databases. In this paper, the authors aim to present a framework to implement the concept of negative database on generic databases (EAV model) for enhancing security. [1]

1.1 EAV MODEL

It is required that whenever logical changes are there in database these changes should be done flexibly without changing the physical structure of database or physical schema of database. For this Entity Attribute Value (i.e. EAV) model of database can be used. The EAV pattern have a simpler approach to database design. It holds everything together in single table, rather than having a different table for each entity and its attributes. In EAV (Entity Attribute Value) model all data can be stored in single generic table with three columns 1 for entity, 1 for attribute and 1 for value as shown in Figure below. This idea was used in various health care database developed in 1970's, after which it is considered in many standard applications like openEHR [02], TMR (The Medical Record), and HELP CDR (Clinical data repository)[1].

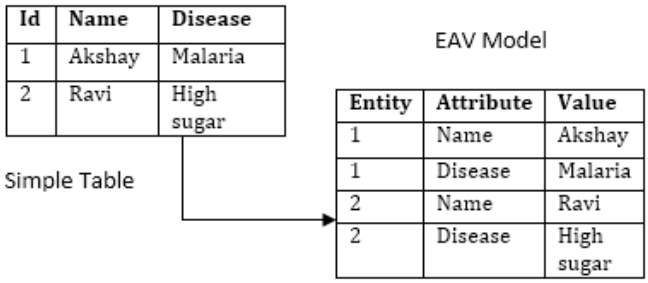


Fig1-Simple Table to EAV Model Conversion

1.2 NEGATIVE DATBASE

Negative Database is concept of adding false data to the original data showing this data along with false data so that if hackers hacks such data then also hacker won't be able to identify the actual data. The negative picture of data records is shown rather than showing the original records. A Negative Database (NDB) can be defined as a database that contains huge amount of data consisting of forged data along with the real data [3]. As stated by Esponda [4], negative database is actually universal set of data minus the positive data of information, i.e., to represent a data field its compliment is used. Basically security using negative database is implemented at middle layer i.e. transport layer where the encryption/decryption and addition of erroneous data take place.

1.3 SHUFFLING

To add one more security layer along with encryption the concept of negative database is used previously [1] the algorithm used to store the false value along with original value stores the original value at fixed position suppose at 'Kth' position. If we want that position variable then we will need to store that value along with the data as another column in the database .Which is similar to the storing of encryption key along with encrypted value which will decrease the security. Another way is to append that value with data itself which will increase algorithms complexity. But if database get hacked then the value of 'k' can give a leak i.e. if hacker gets the 'k' value from every field he can easily get the dataset using decryption. So here by using shuffling algorithm data will be shuffled to change the positions so that no data will be there at their fixed position. This will increase security of data.

2. LITURATURE REVIEW

Implementing security technique on generic database [1]

Provide extra layer of security, negative database has been proposed. Implementation of the negative database on generic databases and have made the sensitive data more secure. The research has succeeded in its aim of providing an extra layer of security to the sensitive information. The main limitation to this algorithm is that the value of variable 'k' is fixed. If we vary the value of k for each entry we have to store it somewhere in order to retrieve the data. If we create another column to store the value of 'k', it will increase the space required and also decrease security.

Negative Database for Data Security [3]

RSA and MD5 algorithms are used for database encryption. Current Timestamp is used for creation negative data. Paper explains concept of storage and retrieval of negative data to the database. But building real world applications can be one of the challenging work because timestamps used for creation of negative database based on the algorithms explained in this paper.

Enhancing Privacy through Negative Representations of Data [4]

The Paper has Negative database concepts based on the binary representation which generate hard-to-reverse NDB. The Paper has two algorithms-1.Prefix algorithm is the first algorithm for generating binary negative databases which is compact and efficient but easy-to-reverse.2 The RNDB algorithm embeds some random factors for generating binary negative databases which are possibly hard-to-reverse but the size of those binary negative databases could be too large. One more disadvantage of the algorithm is some applications which are naturally descripted in real-valued space, the negative database with the binary representation is not appropriate.

File Encryption and Decryption Using Secure RSA [6]

MREA is an asymmetric-key cryptosystem, meaning that for communication, two keys are required: a public key and a private key. Unlike RSA, it is one-way, the public key is used only for encryption, and the private key is used only for decryption. This algorithm also increases the length of private key and hence difficulty to detect the key. Another parameter is modular multiplicative inverse μ where the modular multiplicative inverse μ is new factor of private key, so it will be more difficult to choose μ by trying all possible private keys (brute force attack) hence the security also increases as well as difficulty of detecting the private key.MREA algorithm is used to encrypt files and transmit encrypted files to other end where it is decrypted. The project works efficiently for small size while it consumes time for large size of files.

Real-Valued Negative Databases [7]

Encoding Real Value data in 0's and 1's with some pre-processing then generating binary negative database by using existing algorithm at last decoding the binary negative database to real value negative database [4], Since the data in some applications is naturally represented in real-valued space, it is difficult to apply binary negative Databases properly valued negative database is proposed in this paper. Based on the generation algorithms for the binary negative database, an effective algorithm for generating real-valued negative databases is proposed in this paper. Since the generation algorithm for the real-valued negative database is based on the generation algorithms for the binary negative database, it is always needed to convert real value data to binary to create negative database.

Database Security and Encryption: A Survey Study [8]

Gives Comparison of encryption algorithms and advantages and disadvantages of all encryption algorithms

3. PROBLEM STATEMENT

The security of data is serious issue now a days. Though various cryptographic security techniques, such as hashing algorithms, have already been applied on a database, many cases of unauthorized access to the database are still there. Such unauthorized access can cause misuse of important data. The Proposed system will be using encryption along with the concept of negative database and shuffling of negative data to provide strong layer of security.

4. PROPOSED SYSTEM

The main objective of proposed system is to provide one more layer to the security of the generic database (EAV) model by using concept of negative database which adds false data to original data and shuffling of negative data so that if hackers hack the data they won't be able to get the original data out of false data .The this concept of negative data is used along with the concept of encryption to provide strong security which will be difficult to crack.

4.1 PROPOSED MODEL

4.1.1 STORING DATA IN DATAHASE

While storing data to the database first sensitive and non-sensitive data will be separated and non-sensitive data will be stored directly to the database as it do not require more protection and on other hand sensitive data will passed through the further levels for providing security[1]. At very first level encryption of the data will be performed and cipher text will passed for creation negative data and shuffling module. And finally negative shuffled data will be stored in the database.

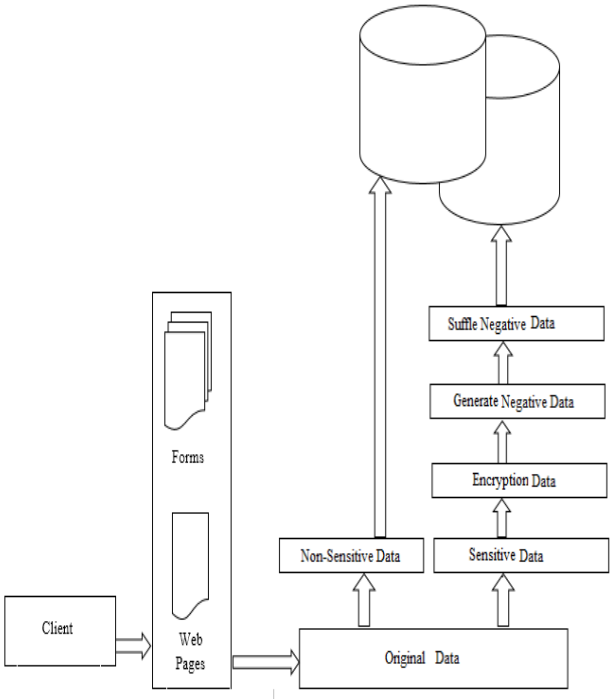


Figure -2: Block diagram of storage of data to the database

4.1.2 RETRIEVING DATA FROM DATABASE

While retrieving data from database non-sensitive data will be directly retrieve by using normal database queries as it will be stored in the database as it is without any processing. But accessing sensitive data will need some preprocessing as it will stored in negative form in the database ,first negative data need to extract from shuffled data and then encrypted data from the negative data .Finally decryption of encrypted data will give us the original sensitive data. At last by combining sensitive and non-sensitive data the final data will be displayed on web page.

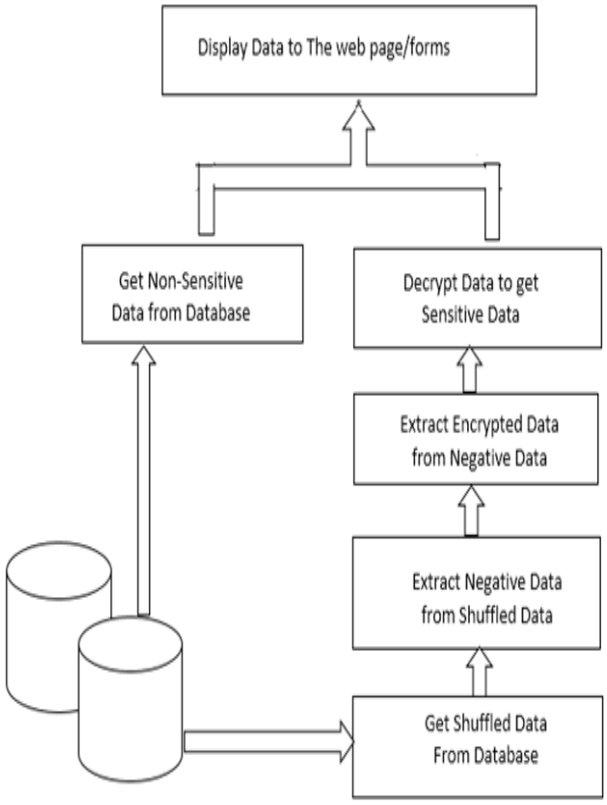
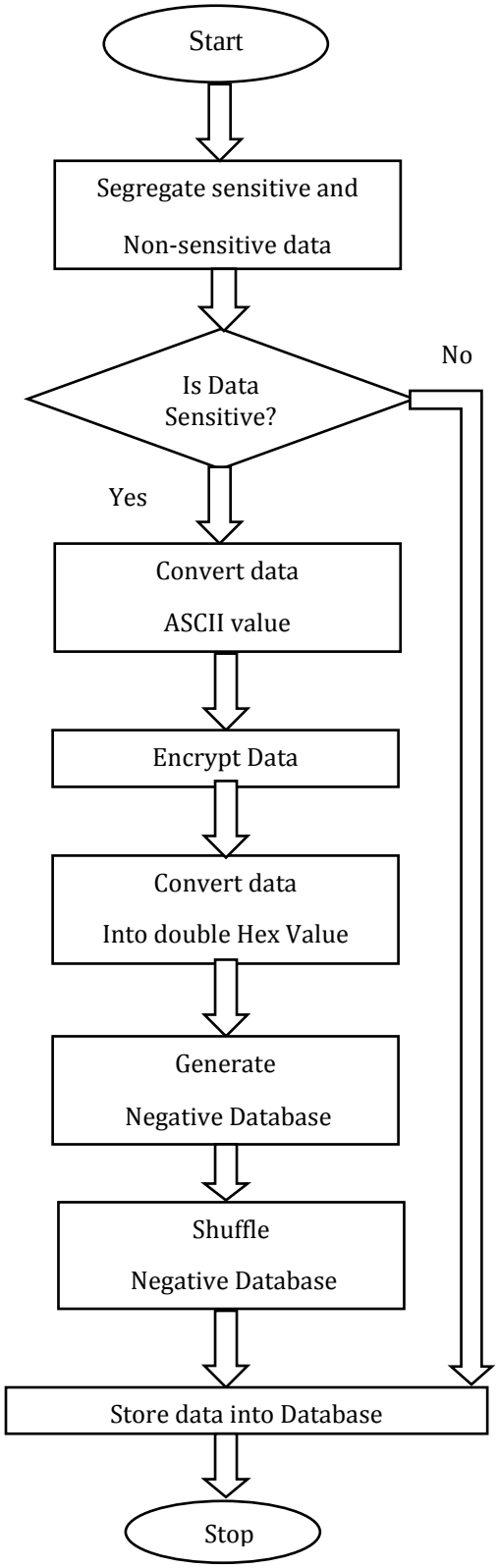


Figure-3: Block diagram of retrieval of data from the database

4.1.3 FOWCHART OF PROPOSED SYSTEM



5. Result

The security system is implemented using concept of negative database so that if someone unauthorized is able to get access of the data then also that person will not able to grab the actual data as data is mixed with huge amount of negative data. While storing data will first separated as non-sensitive data and sensitive data will be further sent through further phases.

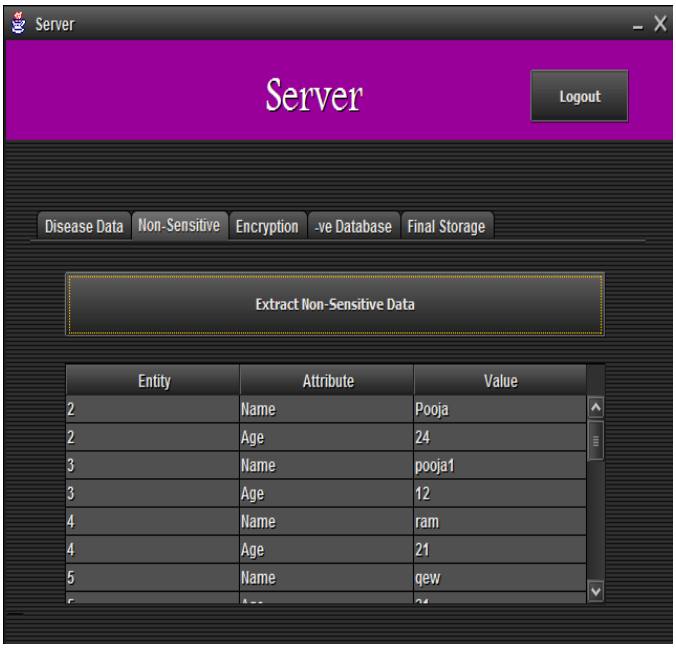


Figure-5: Block diagram of Separating Sensitive and non-sensitive data and displaying non-sensitive data

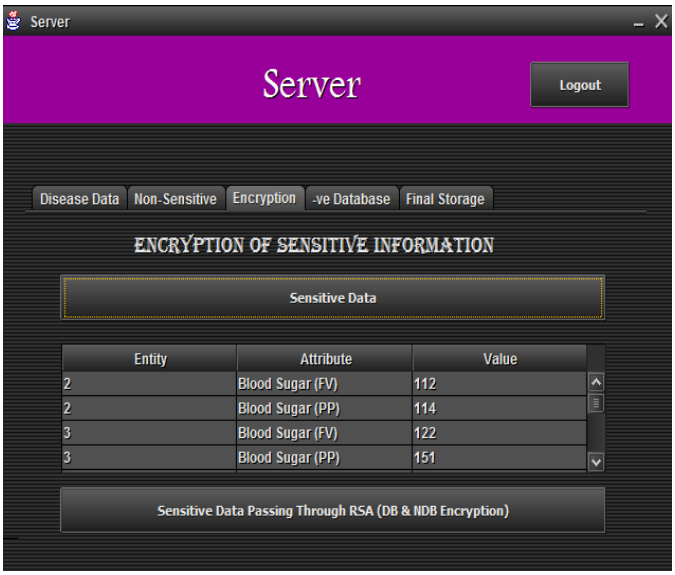


Figure-6: Block diagram displaying sensitive data

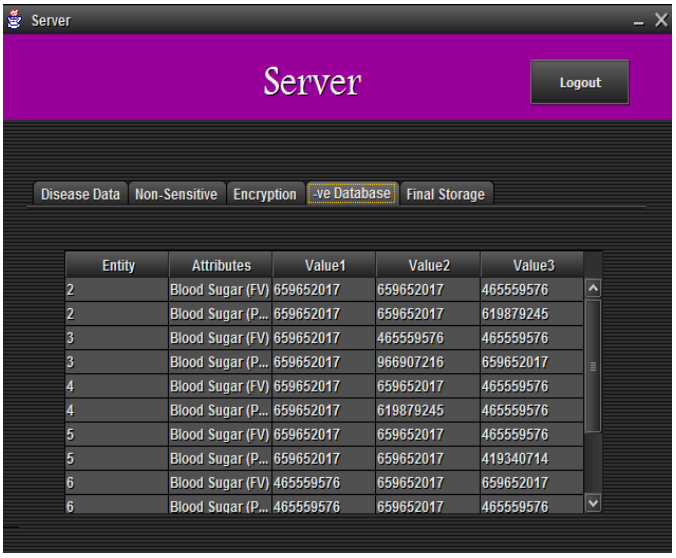


Figure-7: Block diagram generating negative data

6. CONCLUSIONS

Security has always been a domain of active research. The paper uses concept of negative database and shuffling to add more security to user's data keep sensitive data more secure Than previous methods of just using an encryption where hackers can get data by some decryption algorithms. On other hand non-sensitive data is stored in the database as it is. Paper explains example of medical data but concept can be applied in other domain also.

7. REFERENCES

[1] G. Dubey, V. Khurana, S. Sachdeva"Implementing security technique on generic database". Contemporary Computing (IC3), 2015 Eighth International Conference on, Pages: 370 - 376, Year: 2015

[2] www.openEHR.org

[3] Anup Patel, Niveeta Sharma, Magdalini Eirinaki. "Negative Database for Data Security".ICC '09 Proceedings of the 2009 International Conference on Computing, Engineering and Information

[4] Fernando Esponda, Stephanie Forrest and Paul Helman. "Enhancing privacy through Negative representation of data." IEEE, 2002conference.

[5] Daniel Lekberg and Patrik Danielsson "Designing and Implementing Generic database Systems Based on the entity attribute- value Model" thesis Karlstads university.

[6] Rajan.S.Jamgekar, Geeta Shantanu Joshi. "File Encryption and Decryption Using Secure RSA". International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-1, Issue-4, February 2013.

[7] Dongdong Zhao, and Wenjian Luo "Real-Valued Negative Databases", Artificial Immune Systems – ICARIS, 2013

[8] Iqra Basharat, Farooque Azam, Abdul Wahab Muzaffar. "Database Security and Encryption." .International Journal of Computer Applications. Vol. 47(12), June 2012pp. 975 – 888.

[9] Ron Ben-Natan "Implementing Database Security and Auditing",1st Edition.