IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501
Vol.2, No.2, April 2012

Enhanced Privacy Preserving Updates for Anonymous and Confidential Databases

Lavanya.Gunasekaran
SITE, VIT UNIVERSITY
VIT UNIVERSITY
VELLORE, INDIA

R. Sujatha
SITE, VIT UNIVERSITY
VIT UNIVERSITY
VELLORE, INDIA

***Abstract*—** Privacy is main concern in the present technological phase in the world. Information security has become a critical issue since the information sharing has a common need. Thus privacy is becoming an increasingly important issue in many data mining applications in various fields like medical research, intelligence agencies, hospital records maintenance etc. This paper suggests advancing the existing database systems and increasing the security and efficiency of the systems. This paper proposes a new concept to implement a real world anonymous database which improves the secure efficient system for protection of data, restricting the access to data even by the administrator thus maintaining the secrecy of individual patients.

***Keywords*— privacy, database, security, confidentiality, anonymous, cryptography**

I. INTRODUCTION

In today's world databases represent need for increases security. Data in the databases has its own relevant value. For example; medical data collected by over the history of patients over years is an invaluable asset, which needs to be secured and can be used by people in various related areas of work. [1]

Nowadays, privacy accidents have become common problem in the information systems. For example, a hospital may have record of all the patients with various diseases critical and non-critical. If the hospital wishes to reveal the data to any pharmaceutical company or online market services, it should not be able to infer with particularity of patients with those diseases. It can give as a statistical view or just the superficial information such that privacy is not detained.

There are huge numbers of databases that hold numerous confidential information such that people access those data correlating various information from various databases. Access rights for different users must be evaluated and information must be disclosed only to particular extent based on the access rights. Disclosure of confidential information to unauthorized persons may lead to data insecurity leading to dissatisfaction to users. Example privacy accident which occurred so far are numerous. For example, there was a company which sold health products online that also revealed the customer names phone numbers credit card numbers etc on the website. It leads to huge loss of information and breach of privacy. There was another issue when a researcher was enabled to retrieve health records from anonymous databases of insurance claims of employees.

This paper proposes methods to solve the problem of insecurity in database systems by restricting even the administrator from accessing the internal information. The proposed architecture implements the real world anonymous database by implementing the generalization and suppression. It deals with preventing malicious parties and intrusion using encryption and decryption techniques. The efficiency and security of data can be achieved by maintaining single database with specific access rights.

II. RELATED WORKS

In the paper [1] the author suggested paper deals with problems concerning that the users without revealing the contents of tuples and DB, how to preserve data integrity by establishing the anonymity of DB and if the anonymity is authorized then there is a concern of updating the data. It deals with algorithms for database anonymization.

This paper shows how privacy is maintained without disclosing the contents of whole databases and their owner and individual tuples and its owner to eachother.The problem is to check whether the database connecting the tuple is still k-anonymous, such that no one can view the actual data from, tuples or database.

In the paper [2] the author suggests this paper is about k-anonymity in wireless sensor networks (WSN).It has a security framework which has two levels of privacy. In this method, some part of the data is encrypted and the rest of the data is generalized.

In the paper [3] k-anonymity concept has been welcomed in many organizations to release micro data without disclosing identity of persons accessing database. The previous k-anonymity techniques implemented in a common database has breached privacy. It leads to loss of information and privacy accidents. From this first we have to introduce a k-join-anonymity, which allows better effective generalization and helps to diminish the loss of data.

In the paper [4] they discuss the relationship between privacy preserving and SMC and problems involved. It reviews definitions and constructions for secure multiparty computation and discusses the issue of efficiency and demonstrates the difficulties involved in constructing highly efficient protocols.

In the paper [5] the anonymization tables were introduced. The issue of releasing tables mainly in relational

database consisting of confidential data and how it can be resolved, ensuring personal privacy and also maintaining integrity. One of the techniques proposed in the literature is k-anonymization.

It is k-anonymous if the data for an individual person contained can't be eminent from least of k–1 persons all whose data also shows in the same data release.

III. BACKGROUND WORK

A. Basics

The existing system has privacy preserving techniques which can be intruded by various sources and privacy is deterred. The anonymization process and cryptographic techniques are used to enhance the efficiency and protection of confidential information in the databases.

Anonymous database features are either suppressed or they are generalized as far as each row remains identical to at least k-1of the other rows. This is where the database is said to be k-anonymous. The Anonymity thus blocks definite linkages in databases concerning security.

Anonymity gives a definite guarantee that the data is accurately released. The Drawback is the problem of security occurs since the databases are handled by many sources has to be protected.[5]

Cryptographic algorithms and techniques are methods that help to enhance the security of the system and therefore preserve integrity. There are many techniques available in the present technology. The shortcoming of some of the techniques is that they do not provide access rights to the users. Such that for each user has different needs of accessing the database. [6]

The drawback of existing systems is that there is no strong authentication for the systems. If the password for authentication is known to intruder the accounts can't be interrupted and confidential information may be lost. So the authentication should not be able to break even by the administrator, database maintenance, etc.

Moreover, updating of data is a problem in the existing systems due to large amount of data fed in the database. Leads to redundancy and also my lead to loss of valuable information. [6]

Anonymous databases existing do not have proper security and efficiency is low. It can be intruded by various forces. The existing system with cryptographic techniques existing does not grant access rights to the users. [1]

B. Proposed system

The proposed system has features enhanced to existing system. The system is provided with facility for allowing the right users to access into the database by providing username and password and also a random salt value to increase the security and efficiency of the system authentication.

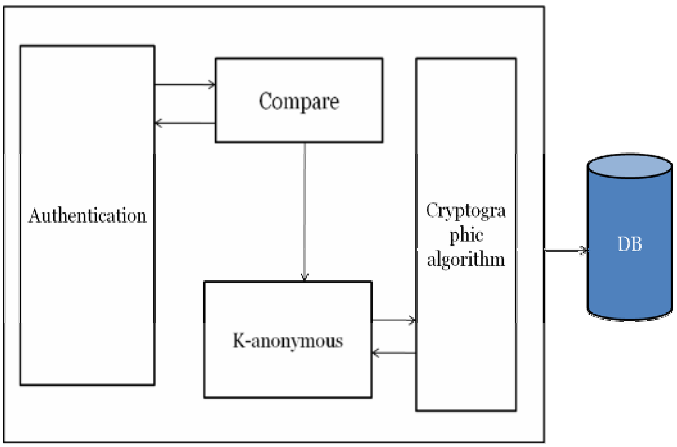

Figure 1: Overview of proposed system

Proposed system in the figure 1 compares existing data and the updates and make sure there is no redundancy and helps to analyses the data in database. K-Anonymization allows database to maintain a suppressed and generalized form of data such that data is much secured. The cryptography technique is used to secure the saved data in database safely such that the information is encrypted, stored and can be retrieved and decrypted back to original with specific authorization.

C. Detailed architectural design

The figure 2 shows the flow of steps followed in the system. It starts with authentication of user. Each user is provided with username and password registered in system already. There is a salt value authentication along with password. The authentication user has access to the database and system has particular access rights for each user. The anonymous database suppresses and generalizes the data according to data value.

The database can be accessed by research centres for gathering statistical data regarding particular medicines, the percentage of curable medicines. The internal or private information of the patients are not revealed to the research centre computation. The research people can see the data's send by the database according to its access right. And allocate research peoples to each research data. And forward the data to research people. Here research people can't do any changes or modifications in patient database they only can use the database for reference purpose.

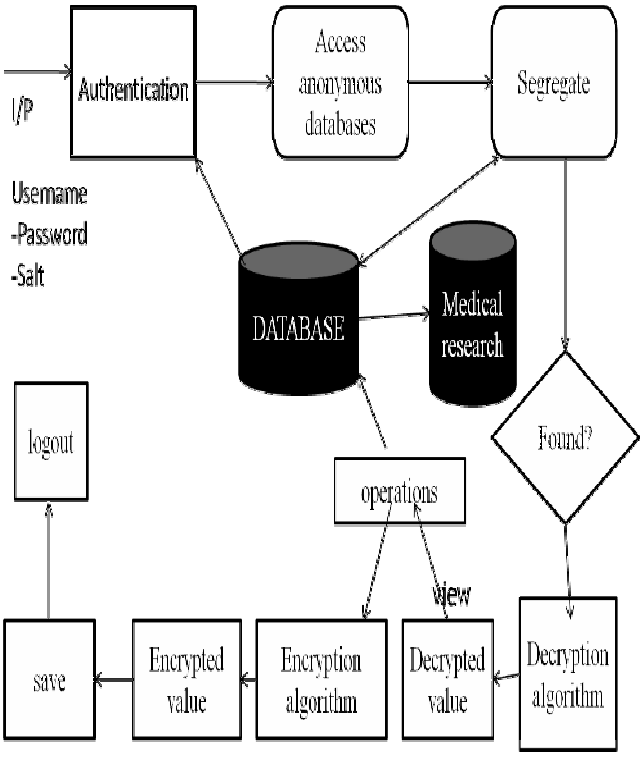

Figure 2: Design view of system.

The authorized database updaters can login into the medical. Here also all the details about the database updater are registered by the admin. And the admin give the authentication details to the particular updater after getting the authentication details, can login to the database and can start the processes.

The doctor and patient enter all details regarding their treatment details in the database in the hospital. These details are not disclosed to the research centre.The data can be encrypted and saved and can be decrypted back to original form when required. [6]

For example, in the proposed system, even the administrator has only restricted access to database, he can't access the internal details of each user, and rather he can find how many users are updated and solve issues regarding users. Individual users are not allowed access to other accounts except their personal record.

Figure 3 shows view of the system for an example patient database where there is a medical database, where the patient registers their details initially. The doctor can view their necessary information about the patient and also fix appointments for patients easily. The patients can in turn fix appointments with their doctor in charge and reduces waiting time for patients due to appointments.

The doctor can in turn update record of patients and their treatments to the patient database. Also the doctor can retrieve information from other sources regarding the illnesses and their treatments.

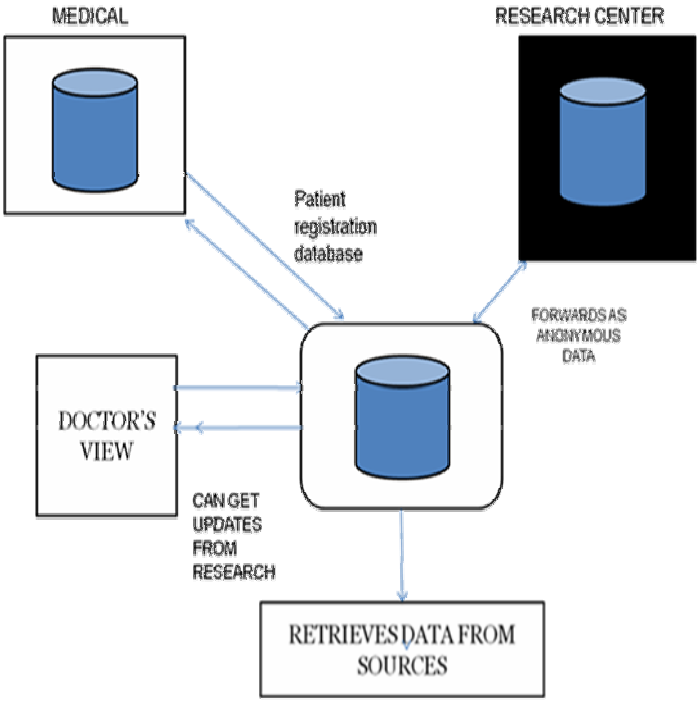

Figure 3: An example diagram of patient database system implementing the idea

The anonymous database can forward information to research centre which has permissions to access the information. The research centre access has its own restrictions for use of the data. They can access only superficial data and whatever data that they have access to. They cannot access the patient details or the particular patient illness.

Figure 4 shows the flow of activities concerning the system. Firstly, the user is authenticated entry into the system. After authentication, according to the user access rights the user can access the anonymous databases in the system. The patient and doctor can perform necessary updates. These data in the anonymous databases can be access by users according to their privileges. The users can access the information from their profile pages. After validating the data and access of data users can close and logout from their account.

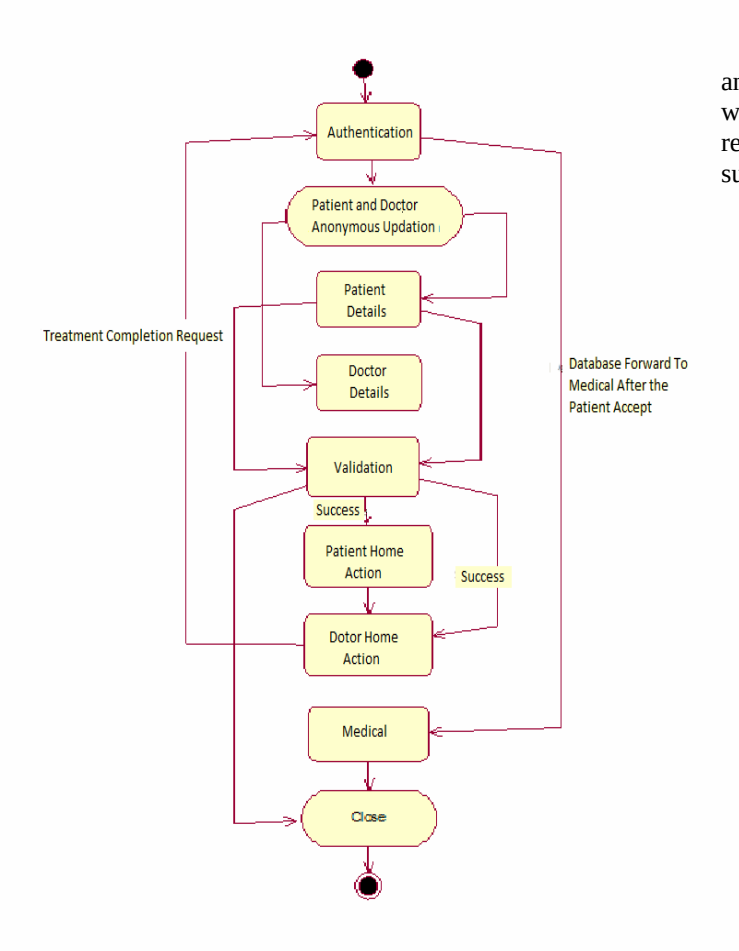

Figure. 4: Example of activity flow of the system

IV. CONCLUSION

This proposed system helps to preserve data for confidential databases. And also helps to maintain privacy and avoid recurring privacy accidents.

The system has various advantages and benefits. Firstly, authentication is improved with username and password and also using a salt value.

Secondly, high privacy of data which updated the approach uses techniques for anonymous data verification and authentication.

Thirdly, Encryption and Decryption techniques help the security. The system proves an efficient protection and security. Moreover, privacy preserved database systems can be achieved to the best. The system encryption, salt value increases security, user satisfaction. [6]

The future work can be enhancing the redundancy of operations and also contriving new private updates to databases that support other notions other than k-anonymity.

ACKNOWLEDGMENT

I am grateful to my university which gave me opportunity and lots of resources to accomplish my project in successful way. Without the guidance of my faculties I would not have reached this far, I thank them all for their timely and scholarly suggestions and motivation.

REFERENCES

[1] Alberto Trombetta, Wei Jiang, Elisa Bertino and Lorenzo Bossi, “Privacy-Preserving Updates to Anonymous and Confidential Databases “2011

[2] Hayretdin BAHS¸˙I, Albert LEV˙I,” k-anonymity based framework for privacy preserving data collection in wireless sensor networks” 2010

[3] R. Agarwal, A. Evfimievski, and R.Srikant, “Information Sharing across Private Databases” ACM2008

[4] Yehuda Lindell and Benny Pinkasy,”Secure Multiparty Computation for Privacy-Preserving Data Mining” 2005

[5] G. Aggarwal, T. Feder, K. Kenthapadi, R. Motwani, R. Panigrahy, D. Thomas, and A. Zhu.” Anonymizing Tables,” Proc. Int’l Conf. Database Theory (ICDT).2004

[6] Anand Sharma and Vibha Ojha,” Implementation of cryptography for privacy preserving data mining” International Journal of Database Management Systems (IJDMS) Vol.2, No.3, August 2010

[7] Mithun Karmakar, Dhruba K Bhattacharyya,” Privacy Preserving Data Mining Using Matrix Algebraic Approach” Department of Computer Science & Engineering, Tezpur University, Napaam, INDIA,doi: 10.4156/jcit.vol4.issue3.5

[8] Andrew Y. Lindelly Making, “Privacy-Preserving Data Mining Practical with Smartcards” 2009

[9] Mr.R.Sugumar Dr.C. Jayakumar, Mr.A.Rengarajan “Design a Weight Based sorting distortion algorithm using Association rule Hiding for Privacy Preserving Data mining” R Sugumar et al, International Journal of Computer Science & Communication Networks,Vol 1(3), 270-276

[10] Xintao Wu, CoPIs: Yongge Wang, Yuliang Zheng. Privacy Preserving Database Application Testing.

CNS-0310974, Sept 15, 2003 to August 31, 2006, NSF

AUTHORS PROFILE

Lavanya Gunasekaran doing her final Year M.S.Software Engineering in School of Information Technology from VIT University, Vellore. Her area of interest includes Network Security, Data Mining and Software Testing.

R.Sujatha received her B.E. degree in computer science from Madras University, in 2001, the M.E. degree in computer science from Anna University in 2009 and currently pursuing the Ph.D. degree in Vellore Institute of Technology, Vellore. She was a lecturer and currently assistant professor, with School of Information Technology and Engineering in Vellore Institute of Technology, Vellore. Her area of research interest includes Data mining, Image Processing and Management of Information systems.