IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 1 (Mar. - Apr. 2013), PP 51-54
www.iosrjournals.org

Suppression and Generalization – Based Privacy Preserving Updates to Confidential Databases

I. Kavitha
Department of Information Technology Rajalakshmi Engineering College, Chennai.

Abstract: *The data owners directly read the contents of the database simply it breaks the privacy of the user's data. If the users access the database content directly then the confidentiality of the data owners has been violated. So both privacy and confidentiality of the database are considered to be a major problem. In the existing system the privacy information gets lost in large amount and does not provide any security mechanism. It is impossible to consider every possible inference and also drastically reduces the quality of the data. The proposed system considers the privacy information is more valuable both in research and business areas. So the data sharing is common in order to provide the data remain k-anonymous even after the updates. The proposed system includes a Commutative Homomorphic Encryption Scheme is used to make the data privacy and confidentiality of the database. This system provides the security of data using RSA algorithm. This system accepts precise inference only and suppresses the sensitive information in order to prevent inference. The proposed system has several important properties which overcomes the drawbacks of the existing system. The properties are anonymous authentication, privacy preservation, confidential access, anonymity maintenance, data management, secure computation, data integrity and also access control.*

Keywords *- Privacy, confidentiality, anonymity, data management, secure computation.*

I. Introduction

The main objective is to check whether the database remain k- anonymous still if a change is been happened to the database and also to make the data Privacy. The proposed system considers privacy information is more valuable both in research and business areas. In the existing system the data owners directly read the contents of the database simply it breaks the privacy of the user's data. If the users access the database content directly then the confidentiality of the data owners has been violated.

In the existing system the privacy information gets lost in large amount and does not provide any security mechanism. The proposed system includes a Commutative Homomorphic Encryption Scheme is used to make the data privacy and confidentiality of the database. This system provides the security of data using RSA algorithm. In the k-anonymity model, privacy protection is achieved by ensuring that every record in a released dataset is indistinguishable from at least (k - 1) other records within the dataset. However, a relevant problem arises when data stored in a confidential, Anonymity-preserving database need to be updated. The operation of updating such a database, e.g., by inserting a tuple containing information about a given individual, introduces two problems concerning both the anonymity and confidentiality of the data stored in the database and the privacy of the individual to whom the data to be inserted. In order to achieve these problems we propose two techniques one is suppression-based and the other one is generalization-based k-anonymous and confidential databases.

Privacy-Preserving Incremental Data Dissemination [4] to identify and prevent data inferences. This paper defines the privacy requirement for incremental data dissemination. And also the attacks are introduced against the anonymization of incremental data. Anonymity for Continuous Data Publishing [1] considers the anonymity problem for a scenario where the data are continuously collected and published. Even if each release is *k* - anonymized, the anonymity of an individual can be compromised by cross-examining multiple releases. Continuous Privacy Preserving Publishing of Data Streams [10] considers the problem of continuous privacy preserving publishing of data streams. This paper identifies the potential applications, to propose a concrete model and an anonymization quality measure, and to develop a group of randomized methods. Empirical evaluation verifies the effectiveness and the efficiency of the methods. This approach is an effective and scalable. The sensitive information of individuals cannot be recovered with high quality. Anonymizing Sequential Releases [5] to study the sequential anonymization problem. Previous works on k-anonymization focused on a single release of data. Privacy-Enhancing k-Anonymization of Customer Data helps [8] to study the concept that how to create *k*-anonymous tables in a distributed scenario without need for a central authority and while maintaining customer privacy.

Anonymzing Tables [3] considers the problem of releasing tables from a relational database containing personal records, while ensuring individual privacy and maintaining data integrity. Anonymous Connections and Onion Routing [6] provide anonymous connections that are strongly resistant to both eavesdropping and

traffic analysis. Database Security – Concepts, Approaches and Challenges [2] provides a complete solution to data security must meet the requirements. This paper helps us to survey the most relevant concepts underlying the notion of database security and summarize the most well-known techniques. Information Sharing across Private Databases [7] tacitly assumes that the data in each database can be revealed to the other databases. Privacy Protection on Sliding Window of Data Streams [9] considers the problem of preserving customer's privacy on the sliding window of transaction data streams. This paper proposes a novel approach, SWAF (Sliding Window Anonymization Framework) is used to solve the problem by continuously facilitating k-anonymity on the sliding window.

II. Proposed Solution

The proposed system provides all the following properties: anonymous authentication, privacy preservation, confidential access, anonymity maintenance, data management, secure computation, data integrity and also access control. In this system, users and surveyor registers with the trusted third party. The trusted third party registers with the admin database. The admin maintains the user records and also categorizes the attributes into sensitive and non sensitive. The user and surveyor communicate with the trusted third party using Commutative Homomorphic Encryption Scheme (CHES). Similarly the trusted third party communicate with the admin using RSA technique. This system ensures the users privacy and confidentiality and also providing security to confidential data. The cryptographic primitives that would be used in the proposed solution are cryptographic hash functions, message authentication, symmetric - key encryption, product-homomorphism and digital signatures.

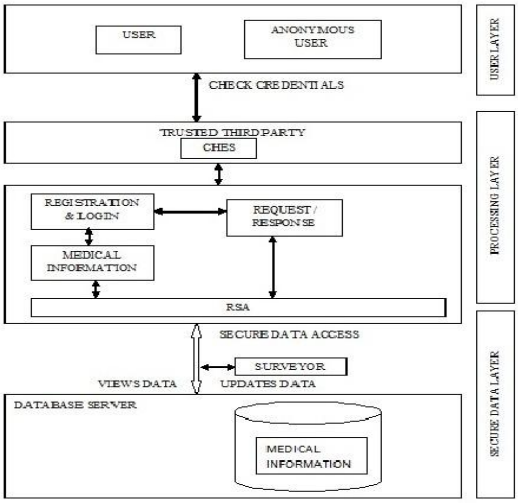

Figure 1. Architecture Diagram

III. An Overview to Confidential Databases

3.1. Administrator

The Administrator will categorize the database attributes into Sensitive and Non-Sensitive. Administrator also maintains all user details and their keys in their database. Also the administrator will mention which are the attributes are more sensitive. The administrator performs user authentication, key issue and service reply. The administrator holds the keys are public key of trusted third party and private key of RSA. The administrator allows the authorized user can view the original database and an unauthorized user can view the suppressed data only. So automatically both the confidentiality of the data and privacy of the user are maintained by the administrator.

3.2. Registration

The Trusted Thirty Party is registered with the Database server and owns its key and also RSA public key, User public key, Surveyor public key. The Surveyor and patients registered with the trusted third party and owns their keys and also trusted third party public key. Administrator (Database server) has trusted third party public key. The user can able to access the data, updating the data and retrieving the data from the database through the trusted third party only.

3.3. Surveyor

Surveyor sends request in the encrypted way to the trusted third party. The trusted third party decrypts and then encrypts the data and sends it to database server. Administrator sends the response in the form of suppressed data to the trusted third party. The trusted third party decrypts and then encrypts the data and sends it to surveyor. The surveyor does the survey and sends the result to the database. The trusted third party decrypts and then updates the database without the knowledge of the administrator.

3.4. User

User sends the request in the encrypted way to the trusted third party. The trusted third party decrypts and then encrypts the data and sends it to database. Administrator sends the response by merging the data to the trusted third party. The trusted third party decrypts and then encrypts the data and sends it to the user. The user view and modify their data and send the result to the research institution for updating into the database. The trusted third party decrypts and then encrypts the data and sends it to research institution. Administrator encrypts the data and updates the patient information.

IV. Privacy Preserving Updates

4.1. Suppression - Based Privacy Updates

With respect to suppression-based anonymization, the database can be classified into two subsets are suppressed attributes and non suppressed attributes. When the tuple T is k-anonymous, then for every tuple t is a subset of the tuple T. In the database the corresponding value is replaced by * (indicating suppressions of the original values). Suppression is used to reduce the content of the database or to minimize the size of the database.

4.2. Generalization– Based Privacy Updates

For generalization-based anonymization, each attribute value can be mapped to a more general value. The main step in most generalization based k-anonymity is to replace a specific value with a more general value. When the tuple T is k-anonymous, they can delete duplicate tuples. After the suppression and generalization, nobody can access the original database.

4.3. System Setup

During setup, the administrator, trusted third party and the user interact as follows.

1) All the systems initialise their state and refresh their memory values.
2) Administrator, trusted third party and user executes message authentication – key generation in order to generate a unique key to encrypt and decrypt the data.
3) Once the keys are exchanged the system setup phase ends.

4.4. Server and Trusted third party Registration

In order to participate in the confidential database system, the server must register server id and their name with the trusted third party. Now the trusted third party registers with the server using server IP address. The trusted third party owns its key, administrator public key, RSA private key and homomorphic private key. Now the trusted third party issues the admin public key to the administrator. The administrator acknowledges the receipt of the details along with the encryption key that will be used to encrypt the data.

4.5. Trusted third party and User Registration

The protocol between trusted third party and user is as follows.

1) The user using its user id such as IP address contacts the trusted third party.
2) The trusted third party verifies its id and connected with the user. Then the authorized user connected with the server through trusted third party. The user owns his private key and trusted third party public key.
3) Then the user can requests the data and retrieves the data from the server through the trusted third party.

4.6. Confidential Connection Establishment

To establish a connection to the server the user must first contact the trusted third party using its id and password. The following steps are carried out during connection establishment.

4.6.1. User validation

The server sends the user status to the trusted third party along with its signing keys. The signing keys are produced by the message authentication code. The authentication algorithms are used to verify the user status that was updated by the server. Then the user public key is displayed in the trusted third party.

4.6.2. Surveyor Updation Process

Surveyor is nothing but the user who wants to make any changes in the database, select the diagnosis before sending the request. Then administrator receives the request with the help of trusted third party. Now administrator sends reply for the response by sending the original message in the secure manner by the use of encryption techniques. The administrator sends the original data by encrypting it with the public key of trusted third party. The trusted third party receives the data from the admin in the form of encrypted message. Third party enters his own RSA private key. Now the trusted third party receives the original message. Then trusted third party enters the surveyor public key and encrypts the message and then sends it to the particular user. Now surveyor receives the encrypted data. And finally the surveyor enters his own private key to decrypt and get the original message. After viewing the original data the surveyor performs changes in the database. Surveyor enters the updating value for the particular diagnosis. Then the surveyor enters the public key of trusted third party to encrypt the updating message. The trusted third party receives the encrypted message. Then trusted third party enters his own homomorphic private key to decrypt and get the original message. After that the trusted third party enters the public key of administrator for updating the database. Updation is done without the knowledge of the administrator. After updating the data in the database, the trusted third party and the surveyor receives the message.

4.6.3. User Process

The user can able to view the data, to update the data and retrieves the data from the database through the trusted third party. During this process the trusted third party uses its own private key, RSA public key and user public key. And administrator needs RSA private key and trusted third party public key. Finally user needs trusted third party public key and user private key.

V. Implementation and Experimental Setup

Using JavaScript to implement the above system was successful due to its in built properties and characteristics. Using SHA-256 for the cryptographic hash functions; HMAC-SHA-256 for the message authentication MA; AES-256 in CBC-mode for the symmetric encryption Enc; and 2048-bit RSA SSA-PSA for the digital signatures Sig. Choosing RSA over DSA for digital signatures because of its faster verification speed—in this system, verification occurs more often than signing was successful.

VI. Conclusion

I have proposed and built a comprehensive credential system, which can be used to make the data privacy and confidentiality of the database. Server can allow only the authorized users to view the original database while maintaining their privacy, and we show how these properties can be attained in a way that is practical, efficient, and sensitive to needs of both users and services. Hope that this proposed work will increase the mainstream acceptance of confidential databases. The proposed security mechanism provides anonymous authentication, data privacy, confidentiality of the data, secure data access, data integrity and access control.

Acknowledgements

I would like to thank Mrs.S.Usha, Assistant Professor (S.S), Information Technology, Rajalakshmi Engineering College, for guiding me in writing this paper.

References

[1]. J.W. Byun, T. Li, E. Bertino, N. Li, and Y. Sohn, "Privacy-Preserving Incremental Data Dissemination", Computer Security vol. 17, no. 1, pp. 43-68, 2009.
[2]. B.C.M. Fung, K. Wang, A.W.C. Fu, and J. Pei, "Anonymity for Continuous Data Publishing", Proc. Extending Database Technology Conf. (EDBT), 2008.
[3]. Y. Han, J. Pei, B. Jiang, Y. Tao, and Y. Jia, "Continuous Privacy Preserving Publishing of Data Streams", Proc. Extending Database Technology Conf. (EDBT),2008.
[4]. K. Wang and B. Fung, "Anonymizing Sequential Releases", Proc. ACM Knowledge Discovery and Data Mining Conf. (KDD), 2006.
[5]. S. Zhong, Z. Yang, and R.N. Wright, "Privacy-Enhancing k-Anonymization of Customer Data", Proc. ACM Symp. Principles of Database Systems (PODS), 2005.
[6]. G.Aggarwal, T.Feder, K.Kenthapadi, R.Motwani, R.Panigraphy, D.Thomas,A.Zhu, "Anonymizing Tables", Stanford University.
[7]. Paul F.Syverson, David M.Goldschlag, and Michael G.Reed, "Anonymous Connections and Onion Routing", IEEE Symposium on Security and Privacy, 1997.
[8]. Elisa Bertino, Fellow and Ravi Sandhu, "Database Security – Concepts, Approaches and Challenges", IEEE Transactions on Dependable And Secure Computing, VOL. 2, NO. 1, JANUARY-MARCH 2005.
[9]. Rakesh Agrawal, Alexandre Evfimievski, Ramakrishnan Srikant, " Information Sharing Across Private Databases", IBM Almaden Research Center 650 Harry Road, San Jose, CA 95120.
[10]. Weiping Wang, Jianzhong Li, Chunyu Ai and Yingshu Li, "Privacy Protection on Sliding Window of Data Streams", Georgia State University.