PUNE RESEARCH WORLD ISSN 2455-359X
AN INTERNATIONAL JOURNAL OF INTERDISCIPLINARY STUDIES Vol 1, Issue 2

PRESERVE THE PRIVACY OF ANONYMOUS AND CONFINDITIAL DATABASE USING K-ANONIMITY

DR. NIKI MALHOTRA
Principal,
College Of Computer Sciences,
Wakad Pune – 57 (MS) (**INDIA)**

ABSTRACT

In field of IT sector to maintain privacy and confidentiality of data is very important for decision making. So there is requirement of certain data to be published and exchanging of the information is in demand. The data to be exchanged contains sensitive information which moves around various parties and this may violate individual's privacy. So to preserve information in its accurate form while moving among various parties, my aim is to provide mechanism knows as k-anonymous technique that doesn't allow the unauthenticated user to modify the data. In this application two protocols that will solve this problem based on suppression and generalization k-anonymous and confidential databases are used. The protocols rely on well-known cryptographic assumptions, and it provides theoretical analysis to proof their experimental results to illustrate their efficiency.

Keywords*: Anonymity, data management, Privacy, secure computation.*

INTRODUCTION

The database is an important asset for many applications and thus their security is important. Data confidentiality is relevant because of the value that data have. As the medical data of patient collected by maintaining the history of patients over several years represent a valuable data that needs to be protected. Due to this requirement gave rise to a large variety of approaches that aim at better protecting data confidentiality and data ownership. Data confidentiality is the problems created by an unauthorized user to get the knowledge about data stored in the database.

Access to individual's personal information is limited by privacy. It deals with the authorized access by authenticated users. Database privacy should follow confidentiality, integrity, and availability of personal data, not only confidentiality alone. Anonymization is required to provide privacy. Anonymization means masking the data. In this identifying information is removed the original data to protect personal or private information. Data Anonymization

allows transferring of information between two organizations, by converting text data in to non-readable form using encryption method. K-Anonymization is one of the approaches that maintain privacy of data. In K-Anonymization approach, at least K-tuples should be indistinguishable by masking values.

The data providers are medical facilities (Hospitals) that provide sensitive information. Through anonymous authentication and connection Authentication is done using user ID and password. The data provider's data privacy is protected from these researchers as the database is in anonymous form.

Literature Survey

In references paper many fundamental methods and techniques are used to make maintain the data of database in anonymous form to provide privacy and confidentiality of data. By performing the literature survey, various issues and challenges are identified in existing system. In 2013, secure protocol is presented for privately checking whether K- Anonymous database remains anonymous even after insertion of new tuple. Quasi-Identifier (QI) [1]: QI is a set of attributes used to identify individual's information. To prevent the attack, masks the values of Quasi-Identifiers using either suppression based or generalization based Anonymization methods. The problem is to check even after connecting the tuple the database is still k-anonymous, such that the actual data from, tuples or database can't be viewed [2]. The same amount of preservation is done for all persons, without considering their needs.

K-anonymity a formal protection model [3] that contains set of accompanying policies for deployment is proposed. K-anonymity protection is provided by release if the information of each person in the release is indistinguishable from at least k-1 individuals whose information is also contained in the release. In 2012, Private Checker's prototype [4] is composed by the modules as: a crypto module that of encrypts all the tuples exchanged between user and the Private Updater, using techniques a checker module that performs all the controls. The Private Checker prototype provides the functionality that check on whether insertion of tuple into the k-anonymous DB is possible. In 2012, the system is provides with facility for allowing the right users to access into the database by comparing existing data and the updates and make sure there is no redundancy and helps to analyses the data in database.

IMPLEMENTATION DETAILS

The information concerning a data provider is stored in single tuple, and DB is kept confidentiality at the server. Since DB is anonymous, the data provider's privacy is protected from researchers. Such task is guaranteed through the use of anonymization. Preserving the privacy & confidentiality without revealing the contents of tuple and DB is done by establishing the anonymity of DB. A secure protocol is presented for privately checking

whether K-anonymous database remains anonymous even after insertion of a new tuple. Suppressed the value of attribute by replacing "*" and Generalized the value with related possible general value to maintain the k-anonymity in database. Thus by making such k-anonymity in table it becomes complicated for third party to identify the record.

PROPOSED MODEL

As shown in fig. 1, proposed system consists of following modules:

a. Login Module.
b. Data Provider for Suppression and Generalization.
c. Server for Suppression and Generalization.

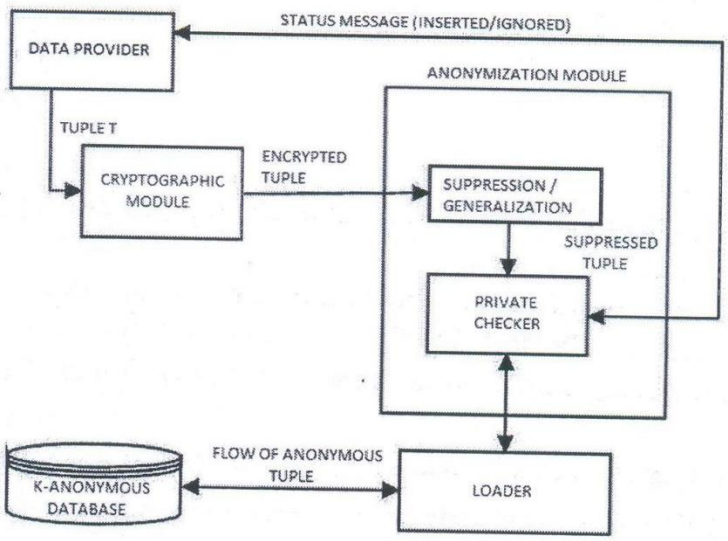

Fig 1. Proposed System Architecture

In this proposed model a secure protocol is presented that privately checks whether database remains k-anonymous even after insertion of new tuple. Quasi-Identifier (QI) : QI is a minimal set of attributes which is used to uniquely identify individuals. Attack is mainly using Quasi-Identifier. Attacks may be re-identification or linking attack. To prevent the attack, masks the values of Quasi-Identifiers using either suppression based or generalization based Anonymization methods. In suppression based anonymization method , mask the Quasi-Identifiers value using a special symbol like * and in generalization based anonymization method , replace a specific value with a more general one using value Generalization Hierarchies(VGH).

The Diffie Hellman key exchange algorithm is used to generate private secure key. Then AES algorithm is applied to encrypt and decrypt data y using the key generated y Diffie

Hellman key exchange algorithm. When user enters his information then this information is encrypted y using AES and also all data in table is encrypted using same algorithm. If information from user matches with tale information the tuple will decrypted and inserted into table.

Conclusion and Future work

Data confidentiality and privacy is a challenging problem faced in case of security of database. In this work, two secure protocols are presented for privately checking whether a K-anonymous database retains its anonymity once a new tuple is being inserted to it. Since the proposed protocols ensure the updated database remains K-anonymous. Thus, by making such K-anonymity in table that makes unauthorized user too difficult to identify the record.

In addition to this, also there are some problems that remained to be addressed:

1) We can improve the efficiency of protocols, by the number of messages exchanged and sizes and algorithm used for encryption and decryption.
2) The private update to database systems techniques supports notions of anonymity different than K-anonymity.

Above are important problems and can be solved in future.

WORKS CITED

1) Sivasubramanian R., K.P. Kaliyamurthie, " Privacy preserving updates to Anonimous databases", IJCSMC,Val 2, Issue 4, April 2013, pg. 582-587.
2) Rajeswari Suryawashi, Prof. Parul Bhanarkar,Rashtrasant Tukdoji Maharaj, "Survey on Privacy Preserving Updates on Anonymous Database", International Journal Engineering Research & Technology (IJERT), Vol 2, Issue 1,January-2013.
3) Mahendrababu P, Rajarajan G,"Apprising in secured Manner to Anonymous and Confidential Databases", International Journal Engineering Research & Technology (IJERT), Vol 2, Issue 1,January-2013.
4) Ebin P. M, Brilley Batley C.," Privacy Preserving Suppression Algorithm for Anonymous Databases" , International Journal of Science & Research (IJSR), Vol 2, Issue 1,January-2013.
5) Mr. Mahesh T. Dhande, Mrs. Neeta A. Nemade, " Performance Improvement of Privacy Preserving in K-anonymous Databases Using Advanced Encryption Standard Technique", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, Issue 6,June-2013.