International Journal of Software & Hardware Research in Engineering
ISSN No: 2347-4890 Volume 2 Issue 12, December-

Privacy Preserving Record Sharing With Anonymous ID Assignment

Prafull B. Masal[1], V. S. Kadam[2]
2 *Associate Professor, Department of Computer Engineering, Sinhgad Institute of Technology, Lonavala 410401, Pune, Maharashtra, India.*
prafull.masal@gmail.com
vsk.sit@sinhgad.edu

Abstract- Algorithm for anonymous sharing of private data among parties is developed. This technique is used iteratively to assign these nodes ID numbers ranging from 1 to M. This assignment is anonymous in that the identities received are unknown to the other members of the group. Resistance to collusion among other members is verified in an information theoretic sense when private communication channels are used. This assignment of serial numbers allows more complex data to be shared and has applications to other problems in privacy preserving data mining, collision avoidance in communications and distributed database access. The required computations are distributed without using a trustedcentral authority.
Existing and new algorithms for assigning anonymous IDs are examined with respect to trade-offs between communication and computational requirements. The new algorithms are built on top of a secure sum data mining operation using Newton's identities and Sturm's theorem. An algorithm for distributed solution of certain polynomials over finite fields enhances the scalability of the algorithms.

Index Terms - Anonymization and deanonymization,

I : INTRODUCTION

Cloud computing is the long dreamed vision of computing as a utility, where cloud customers remotely store their data the cloud so as to enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources. Its great flexibility and economic savings are motivating both individuals and enterprises to outsource their local complex data management system into the cloud. To protect privacy of data and oppose unsolicited accesses in the cloud and beyond it, sensitive data, for instance, e-mails, personal health records, photo albums, tax documents, and so on, may have to be encrypted by data owners before outsourcing to the commercial public cloud; this, however, obsoletes the traditional data utilization service based on plaintext keyword search[1].

Data mining is a technique that helps to extract useful information from a large database. As the amount of data doubles every three years, data mining is becoming an increasingly important tool to transform this data into information. Data mining tools are increasingly being used to infer trends and patterns. The proposed solution guarantees privacy against most of the attacks known to be possible to retrieve private information of individuals. It also provides the necessary patterns to researchers and data miners without deviating from the original data values. Most importantly the solution does not disturb the distribution of the dataset[2].

II: RELATED ARTICLES

Shiba Sampat Kale, Prof. Shivaji R Lahane (1) In this system, stringent privacy is provided by assigning the cloud user a unique ID. This user ID is kept hidden from the cloud service provider as well as the third party user in order to protect the user's data on cloud from the CSP and the third party user. Thus, by hiding the user's identity, the confidentiality of user's data is maintained.

P.Usha, R.Shriram, W.Aisha Banu (2) It was found that through these experiments only a few attributes in the whole dataset are considered to be sensitive. So the key to privacy preservation is to anonymize these sensitive attributes alone and leave the rest. In this model the same is implemented, by anonymizing the sensitive attributes alone and leaving the rest. Finally the whole dataset to k records was anonymized. The software thus successfully implements the aimed privacy measures without disturbing the privacy as well as the distribution of the dataset.

Ankatha Samuyelu ,Raja Vasanth (3) Main focus is on the solution of multi-keyword ranked search over encrypted cloud data (MRSE) while preserving strict system-wise privacy in the cloud computing paradigm.

III: SUMMARY OF EXISTING SYSTEM

Existing and new algorithms for assigning anonymous IDs are examined with respect to trade-offs between communication and computational requirements.. Also, suppose that access to the database is strictly controlled, because data are used for certain experiments that need to be maintained confidential. Clearly, allowing Alice to directly read the contents of the tuple breaks the privacy of Bob; on the other hand, the confidentiality of the database managed by Alice is violated once Bob has access to the contents of the database. Thus, the problem is to check whether the database inserted with the tuple is still k-anonymous, without letting Alice and Bob know the contents of the tuple and the database respectively.

Disadvantage:

The database with the tuple data does not be maintained confidentially.
The existing systems another person to easily access database.
The problem of sharing privately held data so that the individuals who are the subjects of the data cannot be identified has been researched extensively.
The database with the tuple data does not be maintained confidentially.
The existing systems another person to easily access database.
The algorithms for mental poker are more complex and utilize cryptographic methods as players must, in general, be able to prove that they held the winning hand
.

IV: PROPOSED SYSTEM

An algorithm for anonymous sharing of private data among parties is developed. This technique is used iteratively to assign these nodes ID numbers ranging from 1 to N. This assignment is anonymous in that the identities received are unknown to the other members of the group. Resistance to collusion among other members is verified in an information theoretic sense when private communication channels are used. This assignment of serial numbers allows more complex data to be shared and has applications to other problems in privacy preserving data mining, collision avoidance in communications and distributed database access. The required computations are distributed without using a trusted central authority.

Advantage:

The anonymity of DB is not affected by inserting the records.
We provide security proofs and experimental results for both protocols.
The anonymity of DB is not affected by inserting the records.
We provide security proofs and experimental results for both protocols.
That task restricts the level to which can be practically raised. We show in detail how to obtain the average number of required rounds, and in the Appendix detail a method for solving the polynomial, which can be distributed among the participant

V:PROPOSED SYSTEM ARCHITECTURE

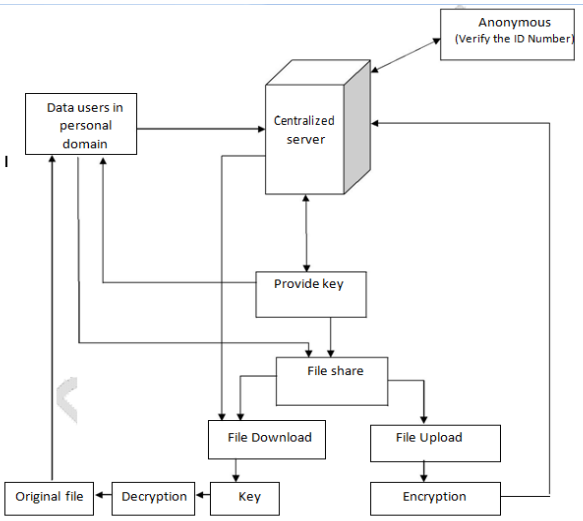

Figure: System Architecture

VI : SYSTEM MODULES

There are four modules:

- Homomorphic encryption Module.
- Generalization Module.
- Cryptography Module
- User and Admin Module.

A: Homomorphic encryption Module:

This module to use the first protocol is aimed at suppression-based anonymous databases, and it allows the owner of DB to properly anonymize the tuple t, without gaining any useful knowledge on its contents

and without having to send to t's owner newly generated data. To achieve such goal, the parties secure their messages by encrypting them. In order to perform the privacy-preserving verification of the database anonymity upon the insertion, the parties use a commutative and homomorphic encryption scheme.

B: Generalization Module:

In this module, the second protocol is aimed at generalization-based anonymous databases, and it relies on a secure set intersection protocol, such as the one found in, to support privacy-preserving updates on a generalization based k-anonymous DB.

C: Cryptography Module:

In this module, the process of converting ordinary information called plaintext into unintelligible gibberish called cipher text. Decryption is the reverse, in other words, moving from the unintelligible cipher text back to plaintext. A *cipher* (or) *cypher* is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a *key*. This is a secret parameter (ideally known only to the communicants) for a specific message exchange context.

D: User and Admin Module:

In this module, to arrange the database based on the patient and doctor details and records. The admin to encrypt the patient reports using encryption techniques using suppression and generalization protocols.

VII: CONCLUSION

In this paper, we studied mainly focused on providing privacy to the data on cloud in which using multi-keyword ranked search was provided over encrypted cloud data using e_cient similarity measure of co-ordinate matching. The previous work also proposed a basic idea of MRSE using secure inner product computation. There was a need to provide more real privacy which this paper presents. In this system, stringent privacy is provided by assigning the cloud user a unique ID.

This user ID is kept hidden from the cloud service provider as well as the third party user in order to protect the users data on cloud from the CSP and the third party user. Thus, by hiding the users identity, the confidentiality of users data is maintained.

VIII: REFERENCES

[1] Shiba Sampat Kale, Prof. Shivaji R Lahane, "Privacy Preserving Multi-Keyword Ranked Search with Anonymous ID Assignment over Encrypted Data" 2014.

[2] P.Usha , R.Shriram "Modified Anonymity Model for Privacy Preserving Data Mining"2013

[3] Ankatha Samuyelu Raja Vasanthi, "Secured Multikeyword Ranked Search over Encrypted Cloud Data".

[4] Jain Wang, Yan Zhao , Shuo Jaing, and Jaijin Le, "Providing Privacy Preserving in Cloud Computing".

[5] Y. Prasanna, Ramesh "E_cient and Secure Multi-Keyword Search on Encrypted Cloud Data".

[6] Larry A. Dunning, Ray Kresman, " Privacy Preserving Keyword Searches on Remote Encrypted Data".

[7] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling E_cient Fuzzy
Keyword Search over Encrypted Data in Cloud Computing".

[8] Ankatha Samuyelu Raja Vasanthi , Secured Multi keyword Ranked Search over
Encrypted Cloud Data, 2012

[9] S. Kamara and K. Lauter, Cryptographic Cloud Storage, Proc. 14th Intl Conf Financial Cryptograpy and Data Security, Jan. 2010.

[10] A. Friedman, R. Wol_, and A. Schuster, Providing k-anonymity in data mining

