International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:268
Vol.2, No.4, April 2013 DOI:10.15693/ijaist/2013.v2i4.18-23

Auxilary Information In Data Privacy And Attacks For Secure Multiparty Protocols

F. Caleb Dany Wesley[1] P. Suresh[2]

[1] PG Student,Sethu Institute of Technology [2]Associate professor, CSE Sethu Institute of Technology

***Abstract*—**Secure multiparty protocols have been proposed to enable noncolluding parties to cooperate without a trusted server. Even though such protocols prevent information disclosure other than the objective function, they are quite costly in computation and communication. The high overhead motivates parties to estimate the utility that can be achieved as a result of the protocol beforehand. In this paper, a look-ahead approach, specifically for secure multiparty protocols to achieve distributed k-anonymity, which helps parties to decide if the utility benefit from the protocol is within an acceptable range before initiating the protocol. The look-ahead operation is highly localized and its accuracy depends on the amount of information the parties are willing to share. Experimental results show the effectiveness of the proposed methods.

***Index Terms*—**Secure multiparty computation, distributed k-anonymity, privacy, security.

I.INTRODUCTION

Multi-party protocols are a basic and important model of communication in any system, practical or theoretical, where there is shared information. The growth of the Internet has triggered tremendous opportunities for cooperative computation, where people are jointly conducting computation tasks based on the private inputs they each supplies. Secure multiparty computation (SMC) protocols are one of the first techniques used in privacy preserving data mining in distributed environments SMP-**Secure multi-party computation** (also known as **secure computation** or **multi-party computation (MPC)**) is a sub field of cryptography. The goal of methods for secure multi-party computation is to enable parties to jointly compute a function over their inputs. Privacy is being alone having your own personal space security is basically knowing your safe and that sure your alone.

We show how look ahead can be extended to enforce diversity on sensitive attributes. To the best of our knowledge, this work is the first attempt in making a probabilistic analysis of k-anonymity given only statistics on the private data.

More specifically, given only statistics on the private data set, we show how to calculate the probability; the probability that a mapping of values to generalizations will make a private data set k-anonymous.

The main focus of this paper is to design the look ahead approach for SMC protocol with the help of distributed k-anonymity technique which is a well-known privacy preservation technique to prevent linking attacks on shared databases. A look-ahead approach is proposed specifically for secure multiparty protocols using the distributed k-anonymity technique. It is used to decide whether the utility benefit from the protocol is within an acceptable range before initiating the protocol. The look-ahead operation is highly localized and its accuracy depends on the amount of information the parties are willing to share the information that they have.

II PROJECT DESCRIPTION

To design the fast look ahead approach based SMC protocol of k-anonymization of horizontally partitioned data. The look ahead returns an upper bound on the probability that k-anonymity will be achieved at a certain utility. Look ahead exploits prior information such as total data size, attribute distributions, or attribute correlations, all of which require simple SMCoperations. Look ahead returns tighter bounds as the security constraints allow more prior information. This is the first work that attempt to make a probabilistic analysis of kanonymity that provides the statistical information about the private data. To design the more secure look ahead protocols using the efficient k- anonymity techniques such as Optimal Distributed k-Anonymization andOptimal Distributed k-Anonymization and Descendant Preserving Distributed k-Anonymization.

III. EXISTING SYSTEM

In existing Method A Look-Ahead Protocol can be implemented. In that system there is database can be split into two database. Based on the user the data can be modified and send to the accessing user. So the data base size will be increase and also updating of the database can be difficult.

In this system the validation of the user can be allotted at particular department only there is no combination and combining of database is not done here. The security constraints allow more prior information. This is the first work that attempt to make a probabilistic analysis of kanonymity that provides the statistical information about the private data. To design the more secure look ahead protocols using the efficient k-anonymity techniques such asDescendant Preserving Distributed k-Anonymization.

***3.1 De Merits*:**

- While these properties are promising for privacy preserving applications, SMC may be prohibitively expensive. In fact, many SMC protocols for privacy preserving data mining suffer from high computation and communication costs.

- The high overhead of SMC protocols raises the question of whether the information gain (increase in utility) after the protocol execution is worth the cost.

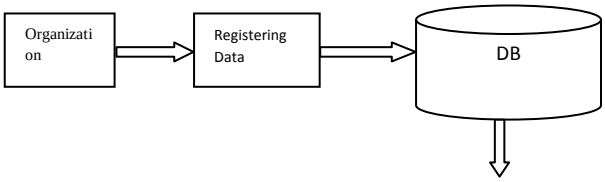
We introduce the Secure Multiparty Protocol System. In this System we develop the Sensitive and non-sensitive Database for access the database. Based on the Access user information can be retrieve for the validation. The access information can be mining and shown to the users only non-sensitive information. The person who are authorized can view the full detail of the data base.

***3.2.1 Meris*:**

- We show how look ahead can be extended to enforce diversity on sensitive attributes.

- To the best of our knowledge, this work is the first attempt in making a probabilistic analysis of k-anonymity given only statistics on the private data.

- More specifically, given only statistics on the private data set, we show how to calculate the probability; the probability that a mapping of values to generalizations will make a private data set k-anonymous.



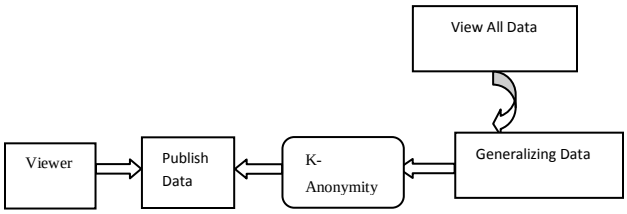


Fig.1 System Architecture

IV MODULES

Secure Multiparty Computation:

Secure multiparty computation (SMC) protocols are one of the first techniques used in privacy preserving data mining in distributed environments. While doing so, the protocol does not reveal. Anything other than the output of the function or anything that can be computed from it in polynomial time.

Multiparty secure computation allows N parties to share a computation, each learning only what can be inferred from their own inputs and the output of the computation. For example, the parties can compute summary statistics on their shared transaction logs, including cross-checking of the logs against counterparties to a transaction, without revealing those logs.

Our focus is the SMC protocol for distributed k-anonymity previously studied. K-Anonymity is a well-known privacy preservation technique proposed in to prevent linking attacks on shared databases. Linking attacks are performed by adversaries who know some attributes (quasi-identifier attributes) of an individual to identify him/her in the data set. A database is said to be k-anonymous if every tuple projected over the quasi-identifier attributes appears at least k times in the database.

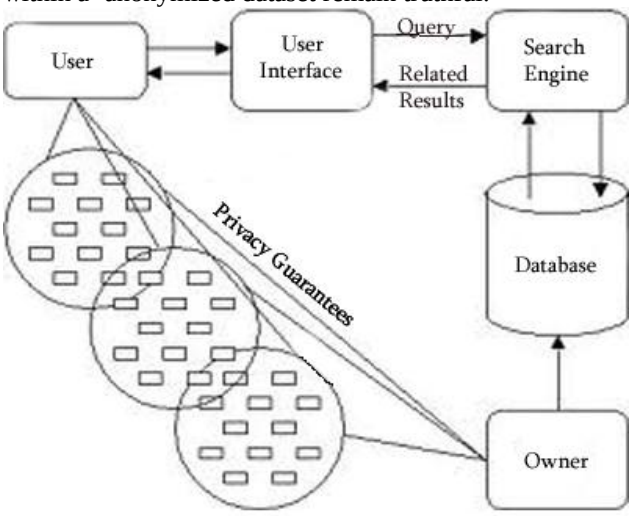
Look-Ahead Approach

We introduce and formally define secure look-ahead protocols. We design a fast look ahead of k-anonymization of horizontally partitioned data. The look ahead returns an upper bound on the probability that k-anonymity will be achieved at a certain utility. Utility is quantified by commonly used metrics from the anonymization literature. Look ahead exploits prior information such as total data size,attribute distributions, or attribute correlations, all of which require simple SMC operations. Look ahead returns tighter bounds as the security constraints allow more prior information. We show how look ahead can be extended to enforce diversity on sensitive attributes as in the format.

To the best of our knowledge, this work is the first attempt in making a probabilistic analysis of k-anonymity given only statistics on the private data. More specifically, given only statistics on the private data set, we show how to calculate the _-probability the probability that a mapping of values to generalizations will make a private data set k-anonymous.

K – Anonymity:

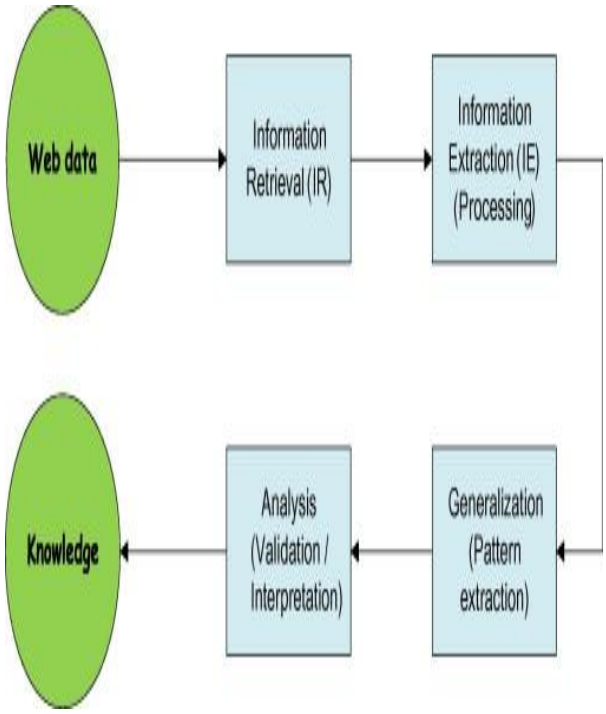
The process of -anonymizing a dataset involves applying operations to the input dataset including data suppression and cell value generalization. Suppression is the process of deleting cell values or entire tuples. Generalization involves replacing specific values such as a phone number with a more general one, such as the area code alone. Unlike the outcome of other disclosure protection techniques that involve condensation data scrambling and swapping or adding noise all records within a -anonymized dataset remain truthful.



The problem of -anonymity is not simply to find any -anonymization, but to instead find one that is "good" according to some quantifiable cost. The problem of optimal -anonymity is to find one that is known to be "best."

Generalization:

Data Generalization is the process of creating successive layers of summary data in an evolutionaldatabase. It is a process of zooming out to get a broader view of a problem, trend or situation. It is also known as rolling-up data.We assume data are horizontally partitioned. A look ahead on vertically partitioned data involves a comparative quantification of utility over different projections of the data set thus requires the design of correlation aware cost metrics. We leave such an analysis as a future work and focus on horizontally partitioned data sets.



5.RESULTS

Most SMC protocols are expensive in both communication and computation. They introduced a look-ahead approach for SMC protocols that helps involved parties to decide whether the protocol will meet the expectations before initiating it. They presented a look-ahead protocol specifically for the distributed k-anonymity by approximating the probability that the output of the SMC will be more utilized than their local anonymizations. Experiments on real data showed the effectiveness of the approach. Designing look aheads for other SMC protocols stands in this work.

Fig 2. Home Page

The above Fig 2 Mentioned to display the hospital website

DOI:10.15693/ijaist/2013.v2i4.18-23

Fig 3. Registration

The above figure is mentioned for creating the account for Doctor and also for the Patient, this will get stored in the database of the particular hospital.

Fig 4. Doctor Registration

The above figure shows the full process of doctor registration,It will get the complete details about the doctor.

Fig 5. Generalization

The above figure is shows the process of generalization for the doctor, this will ask the doctors to choose the fields for the generalization.

Fig 6.Patient Registration

The above figure mentions the complete process of the patient registration, gets the patients details and store it in the hospital database where it belongs.

Fig 7.User Login

The above figure mention the process of login as a patient&doctor into the Hospital Database, this will identifies the authorized and unauthorized persons.

Fig 8.Generalized View

The above picture mention the generalized view for the unauthorized persons, the sensitive data's are hidden using '*' so that the un authorized persons are prevented.

Fig 9.Full Authorized view

The above figure mention the complete view for the authorized person, only the doctors can view the sensitive data.

6.CONCLUSION

Most SMC protocols are expensive in both communication and computation. They introduced a look-ahead approach for SMC protocols that helps involved parties to decide whether the protocol will meet the expectations before initiating it. They presented a look-ahead protocol specifically for the distributed k-anonymity by approximating the probability that the output of the SMC will be more utilized than their local anonymizations. Experiments on real data showed the effectiveness of the approach. Designing look aheads for other SMC protocols stands as a future work. A wide variety of SMC protocols have been proposed especially for privacy preserving data mining applications each requiring a unique look ahead approach. As for the look-ahead process on distributed anonymization protocols, definitions of k-anonymity definitions can be revisited, more efficient techniques can be developed and experimentally evaluated.

7.REFERENCES

[1] R.J. Bayardo and R. Agrawal, "Data Privacy through Optimal KAnonymization,"Proc. 21st Int'l Conf. Data Eng. (ICDE '05), pp.217-228, 2005.

[2] C. Blake and C.J. Merz, "UCI Repository of Machine Learning Databases," http://www.ics.uci.edu/mlearn/MLRepository. html, Univ. of California, Irvine, Dept. of Information and Computer Sciences, 2012.

[3] B.-C. Chen, K. LeFevre, and R. Ramakrishnan, "Privacy Skyline: Privacy with Multidimensional Adversarial Knowledge," Proc. 33rd Int'l Conf. Very Large Data Bases (VLDB '07), pp. 770-781, 2007.

[4] J. Domingo-Ferrer and V. Torra, "Ordinal, Continuous and Heterogeneous K-Anonymity through Microaggregation," Data Mining and Knowledge Discovery, vol. 11, no. 2, pp. 195-212, 2005.

[5] W. Feller, An Introduction to Probability Theory and Its Applications, vol. 1, Wiley, 1968.

[6] S.R. Ganta, S.P. Kasiviswanathan, and A. Smith, "Composition Attacks and Auxiliary Information in Data Privacy," Proc. 14th ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining (KDD '08), pp. 265-273, http://doi.acm.org/10.1145/1401890. 1401926, 2008.

F. Caleb DanyWesley received his B.E degree in Computer Science Engineering from Kalasalingam University,Krishnankovil, Tamil Nadu in 2011. Currently he is pursuing his M.E (CSE) from Sethu Institute of Technology, Kariyapatti, VirudhunagarDist.,Tamil Nadu, India.

His research interests include Networking, Data Mining, and Mobile Computing.