Secure Multi Party Computation For Participating Parties

Ruby S, Mr Raja Varman
M-Tech, Computer Science and Engineering
Dr. MGR Educational and Research Institute University.
Chennai-6000095, India.
Assistant Professor, Computer Science and Engineering
Dr. MGR Educational and Research Institute University.
Chennai-6000095, India.

***Abstract*— In this paper secure multi party computation parties together compute their private inputs, same time these inputs are kept secured. We also propose SMC problems along with some solutions. It provides detailed work conclusion about SMC. Therefore, keeping the data together and provide collaborate computations without revealing data of individual.**

***Keywords*— Security, Trusted Third Party, Secure Multiparty Computation.**

I. INTRODUCTION

Internet and distributed computer provides joint computations. SMC is a mechanism is used for joint computations in distributed environment. It can be defined as, to provide computations in a secure manner. With SMC, parties can perform global computation on their private data without loss of data. It provides secure multiparty protocol development. Secure multi-party computation has an answer to this problem. Informally, if a protocol meets the SMC the parties learn only the final result. An example is millionaire problem, two millionaires, Sam and nice, want to learn who is richer without disclosing their actual wealth to each other. the research community has developed SMC protocols, for applications as forecasting, decision tree analysis and auctions among others.

The SMC model does not guarantee that data provided by parties are truthful. In many situations, data needed for building data analysis are distributed among multiple parties with interests. For example, a credit card company analysis that credit card fraud may increase its profits as compared to its peers. In SMC, participating parties provide truthful inputs. This is justified by the fact that learning the correct data is the interest of all participating parties. SMC protocols require expensive computations, if any party does not wish to know the results, the party should not participate. Still, this does not guarantee the truthful result of the private data when parties wish to learn the final result. SMC guarantee that nothing other than the final analysis result is revealed, it is impossible to verify parties are truthful about their private input data. SMC techniques cannot prevent input modification by parties.

SMC provides a framework that transforms a normal computation to Secure multi party computation .the number of inputs, we can classify the computations into single input and multi-input. This can be viewed as a drawback as all the computations may demand the same security. Therefore, there is a need to distinguish SMC computation and other computations can be carried out normally. SMC done in the form of database, authentication validations, mathematical and relational, scientific and statistical computations and geometrical operations. Several problems can be viewed as SMC problems. We have listed many SMC problems and provide some new SMC problems and their applications along with the solutions

II. BACKGROUND AND RELATED WORK

Large numbers of work has been done on SMC to provide secure computations.This computation can be like selective

information sharing, arithmetic, relational operations, sorting, searching, hashing and other operations. *Database Query*: Suppose Sam want to search in Nice database and it just want to return the result, without revealing the Nice entire database. The match could be exact or approximate match.

Profile Matching: Sam has a database of hacker's profile. Nice has recently traced a behaviour , whom he suspects a hacker. Now, if Nice wants to check whether his doubt is correct, he needs to check Sam's database. Sam's database needs to be protected because it contains hacker's related information. when Nice enters the hacker's behaviour and searches the Sam's database, he can't view his behavor database, but only gets the comparison results of the behaviour.

Fraud Detection: Two major health organizations wish to cooperate in preventing fraudulent into their system, without sharing their data patterns, since their individual database contains sensitive data.

Classification: Sam has a private database K1 and Nice has private database K2. How can Sam and Nice build a decision tree based on K1 ∪ K2 without disclosing the contents of their private database to each other? algorithms like ID3,Gain Ratio, Gini Index can be used for Decision Tree along with SMC.

Data Clustering: Sam has a private database K1 and Nice has private database K2. Sam and Nice want to jointly perform data clustering on K1 ∪ K 2. This is primarily based on data clustering to increase similarity and minimize similarity.

Mining Association Rules: Let Sam has a private database K1 and Nice has private database K2. If Sam and Nice wish to jointly find the association rules from K1 ∪ K 2 without revealing the information from individual databases.

Data Generalization, Summarization and Characterization: Let Sam has a private database K1 and Nice has private database K2. If they wish to jointly perform data generalization, summarization and characterization on their combined database K1 ∪ K2, then this problem becomes an SMC problem.

Intersection: Let Sam has a private shape a and Nice has private shape b, if Sam and Nice want to find whether a and b intersect, then they need to share their database to find whether they intersect.

Point Inclusion Problem: Let Sam has a private shape a and Nice has private point p. Now, if Nice wish to know whether his private point p lies on shape boundary or inside and outside, then they need
to jointly use both databases without telling their individual information to each other.

Range Searching: Let Sam has a private range and has Nice private points. Sam and Nice want to jointly find the number of points in the Sam's range; neither is willing to revel their data to other party.

Closest Pair: Let Sam has M private points and Nice has N Private points in a plane. Sam and Nice want to jointly find the two points closest among (M+N) points, i.e. two points having their mutual distance .

Convex Hull: Sam has M private points and Nice has N Private points in a plane respectively. They wish to find a convex hull from these (M+N) points.

Selection Problem: Let Sam and Nice have their own private databases. If they want to apply any selection procedure on each other's databases, then such a process should not disclose their database knowledge to the other party.

Sorting Problem: Let Sam and Nice have their private databases and they jointly want to sort their database without revel each others database.

Shortest Path Problem: Let Sam and Nice both have their location databases and they wish to find the shortest path among the two locations a and b.

III. SMC PROBLEMS AND SOLUTIONS

The research universities from various countries wish to invent some current research trends from their research data without compromising the security of each individual data.

Consider that several shopkeepers of some general stores wish to find shopping of customers and buying patterns without revealing information about their data.

Consider an Intelligence Agencies that considers database of fingerprints and thumb impressions. Now, if somebody from police station wishes to check a particular fingerprints, it must not be able to gain its complete access, instead, he should only get the test results.

If police wishes to check a particular person's identity from his thumb impression and signature, they can consult the bank database. Bank database only disclose the match results of thumb impression and signature.

Let all universities across the globe wish to evaluate each other and then declare the top universities of the world on the basis of their 5 year's academic records. They all wish to preserve the privacy of their individual databases.

Consider hospitals situated in various different countries having their medical databases ,patient's history stored on some remote database sites. If an insurance company want to verify the particular person and he can get that patient's information from the hospital and but the hospital does not provide the information of the person and only the requested information is allowed to operate .

Let all doctor's team from several countries wish to find a remedy for a disease. All of them carry out research and studies and only reveal conclusions before each other without revealing the whole task.

Consider Airlines that has a reservation database for each country. If a person wants to make a reservation from city A located in country A to a city b located in country B and then we need to consult each countries databases. These data provide only the queried details without disclosing their whole reservation database.

A social organization providing funds to large number of charitable trusts located in different countries. These trusts can query the organization to check whether the requested fund has been issued or not and cannot see the organization's whole database.

Several websites provides ocean of knowledge and contains authentication information. Whenever, we do e-shopping /e-commerce, the authentication database first validates us as an authenticated user and then when it comes to payment and our account number and credit card number is checked for correctness in the bank database and if transaction successfully completes and then only item is said to be purchased. In this, authentication checks the individual person's identity and bank's database check the card number only and other authentication and the bank database is kept confidential.

Cryptographic : In this, the input from several parties in received in encrypted form by Trusted Third Party.

Randomization : In this the input from several parties is first concatenated and associated with a random number, in order to keep it secure.

IV. CONCLUSION

This paper brings several SMC problems and their solutions to light such as database queries and intrusion detection and geometric computation and Statistical Analysis and Scientific Computation. Researches are still to get efficient solutions to all the SMC problems and as the scope of the SMC are growing and this area is gaining a lot of interest and attention. With use of computers, proliferation of sensitive and private data is very important. The aim of this paper is to divert the attention of the people who work even in other computation areas to view computation problems as SMC problems and suggest solutions for the same. Although much of this paper can be read with very little background in cryptography, we assume familiarity with basic concepts like "computational indistinguishable" when we present the formal definitions. An excellent survey by Goldreich provides all of the background necessary for reading this and more advanced papers. For those interested in going a step further, we recommend for a general introduction to cryptography, and for a rigorous and in-depth study of the foundations of cryptography.

REFERENCE

[1] D.K. Mishra and M. Chandwani,"Anonymity Enabled Secure Multiparty Computation for Indian BPO". In Proceeding of the IEEE Tencon 2007: International conference on Intelligent Information Communication Technologies for Better Human Life, Taipei, Taiwan on 29 Oct. - 02 Nov. 2007, pp. 52-56.

[2] Rebecca Wright, "Progress on the PORTIA Project in Privacy Preserving Data Mining," A data surveillance and privacy protection workshop held on 3rd June 2008.

[3] Wenliang Du and Mikhail J. Atallah,"Secure Multiparty Computation Problems and their Applications: A review and Open Problems," Tech. Report CERIAS Tech Report 2001-51, Center for Education and Research in Information Assurance and Security and Department of Computer Sciences, Purdue University, West Lafayette, IN 47906, 2001.

[4] Jaideep Vaidya and Chris Clifton, "Leveraging the 'multi' in Secure Multiparty Computation," WPES'03 October 30, 2003, Washington, DC, USA, ACM Transaction 2003, pp120-128.

[5] Andrew C. Yao,"Protocols for Secure Computations", In Proc. 23rd IEEE Symposium on the Foundation of Computer Science (FOCS), IEEE 1982, pp 160-164.

[6] Chris Clifton, Murat Kantarcioglu, Jaideep Vaidya, Xiaodong Lin, Michael Y. Zhu, "Tools for Privacy Preserving Data Mining". international conference on knowledge discovery and data mining, Vol. 4, No. 2, 2002, pp. 1-8.

[7] Vassilios S. Verykios, Elisa Bertino, Igor Nai Fovino, Loredana Parsiliti Provenza, Yucel Saygin, Yannis

Theodoridis, "State-of- The-Art in Privacy Preserving Data Mining", SIGMOD Record, Vol. 33, No. 1, March 2004.

[8] Y.C.Yao, "How Generate and Exchange Secrets". In proceedings of the IEEE Symposium on Foundation of Computer Science IEEE, 1986, Pages 162-167.

[9] O.Goldreich, "Secure Multiparty Computation", September 1998 (Working draft) Online available on: http://www.wisdom.weizmann.ac.il/~oded/pp.html.

[10] R.Agrawal and R.Srikant, "Fast Algorithms for Mining Association Rules", in the proceedings of the 20th International Conference on Very Large Databases (VLDB), Santiago, Chile, September 12-15 1994.

[11] Y.Lindell and B. Pinkas, "Privacy Preserving Data Mining". In advances in Cryptography-CRYPTO-2000, pp 36-54, Springer- Verlag, August 24 2000.

[12] Y.Lindell, IBM T J Watson "Tutorial on Secure Multiparty Computation", available on wesite:- http://www.cs.biu.ac.il/~lindell/research-statements/tutorials-