World of Computer Science and Information Technology Journal (WCSIT)
ISSN: 2221-0741
Vol. 1, No. 5, 198-201, 2011

Hybrid Technique For Secure Sum Protocol

Ms. Priyanka Jangde
Information Technology Department
SSSIST,
Sehore, India
priyankajangde@gmail.com

Mr. Gajendra Singh Chandel
Information Technology Department
SSSIST,
Sehore, India
Gajendrasingh86@rediffmail.com

Mr. Durgesh Kumar Mishra
Department of Computer Science &
Engineering AITR,
Indore, India
durgeshmishra@ieee.org

Abstract— Secure Multiparty Computation (SMC) allows parties to compute the combine result of their individual data without revealing their data to others. Secure sum computation is one of the important tool of the SMC. On SMC many eminent researchers give their protocols especially in secure sum computation, researchers show their interest. In this paper we provide unique hybrid protocol for secure sum computation which is the combination of Ideal and Real Model. This protocol provides *zero data leakage* means it is completely secure. If two or more than two parties including third party (TP) become malicious cannot hack or trace the data of any other parties, who were participating in this computation. With the help of Hybrid model we are enhancing the security of the computation and maintaining the privacy of the data. In this paper, we analyzed the computational and communicational complexity and found that both the complexities are O (n).

Keywords- Secure Multiparty Computation (SMC); Third Party (TP); Secure Sum Protocol; Hybrid.

I. Introduction

Secure Multiparty computation problem is not a problem of single party as the name itself says it is the problem of multiple parties' i.e. n parties. In SMC problem, n parties want to compute their private data or function as input in secure mode means data of individual party cannot be disclose or reveal to other and correct result is computed. During secure sum computation security is required because it may be possible some of the parties act as malicious and misuse other parties' data. In secure sum computation at present there are two models Ideal model and Real model, secure sum concept uses real model.

In Ideal model third party perform computation we assume that it is trusted and whole computation is done by Trusted Third Party (TTP), parties send their data in secure mode to TTP. Numbers of protocols are proposed by researchers for this model. Other than this Real model don't use TTP for computation. Computation is done by parties itself, Party share their data with each other in secure mode i.e. party either encrypt their data or splits their data in segments many more techniques are proposed by many researchers for sharing data with each other or with TTP in both the models.

There are so many practical examples where privacy of data is main concern. One of them is in insurance companies, when they want to calculate how many persons are insured and don't want to reveal their number of customers. With the secure sum computation total number of persons insured is calculated. Our proposed Hybrid model is inspired with both the real and ideal models. In Hybrid model computation is done by parties and third party. Both do computation at their end according to algorithm proposed.

II. Literature Survey

SMC problem was introduced by Yao in 1982[1]. He proposed well known millionaire problem. In this problem two millionaires wanted to know who is richer among them without disclosing their wealth to each other. The solution provided by Yao was for semi honest. Semi honest parties' means they want to know other information also. Then Clifton et al introduce tools for privacy preserving distributed data mining [13]. He gave four efficient methods for privacy preserving computation that can be used to support data mining. All four are not truly secure multiparty computation. Secure Sum is one o them and it is secure multiparty computation. The SMC problem is further extended by Goldrich et al [4]. They used circuit evaluation protocols for secure computation. All these are the theoretical aspects of SMC. After theoretical studies few practical problems of SMC was introduced i.e. Privacy information retrieval problem (PIR), Privacy preserving Statistical analysis, Privacy Preserving Scientific Computation, Privacy preserving Data Mining, Privacy Preserving Geometric Computation etc. In PIR problem there is a client and a server, client want to hack the ith it from the server without letting know I to server and server does not want that client ever know the binary sequence. Beside this, Lindall et al [2] and Agrawal et al [3] respectively provide cryptographic technique and solutions for SMC and for mining association rule, provide fast and secure algorithm. For routing and other related problems Atallah et al [11] gave their contribution to secure multiparty computation geometry. Through PORTIA project of Rebecca Wright some of the problems of SMC and privacy preserving data mining got the solution. Many eminent researchers provided their views and solutions of problems for SMC.

After all this new researchers came in light with their new ideas and concepts for SMC. Mishra et al [15] worked and gave many protocols for ideal model of SMC. They gave multilayered protocols. In starting they proposed two layered architecture and protocol for implementation. The improved version of two layered protocol is three layered protocol. In this protocol third layer is added between participating parties' layer and third party layer called anonymizer layer. The purpose of anonymizer layer is to hide the identity or information of the parties from the third party. Then this three layer protocol is improves by four layered protocol in which packet layer was added. This packet layer is added for providing security to the data from the intruders and malicious parties or activities; this is helpful if third party is not trusted.

After this Sheikh et al [16] worked on the real model of SMC. In which they proposed many protocols for secure sum computation. In these protocols they used random numbers for privacy of input data of individual parties. Individual party input data is divided into number of segments so that data leakage reduces. The number of data segments is inversely propotional to the leakage of data.

There are some loop holes and constraints in previous works to remove those problems we proposed a new protocol which is the combination of two, ideal model and real model, named as Hybrid model. We extend secure sum computation with Hybrid model to increase security and privacy of data.

III. Proposed Hybrid Technique of Secure sum Protocol

The proposed Methodology is concept of secure Sum computation. In our protocol other than existing model protocols different idea is proposed which is the combination of Ideal and Real model, named Hybrid model. In this protocol n parties and one third party exist. N Parties compute the Sum of their data with the help of third party. Third party is not trusted so for privacy and security of data, data is divided into segments. Segment of the data is done on the parties side, no method is proposed for the segmentation of data, it is on party how they divide their data in segments only number of segments is previously announced . All party divides their data in three segments. Computation of these segments is done by communication between parties and third party. For more security and privacy random numbers are added with the segments. After computation of sum result is announced by third party to all the parties.

IV. Informal Description

In this protocol Hybrid model of secure Sum Computation is proposed as shown in figure 1. In Hybrid model third party and individual parties both do computation partially at their end. In this protocol each party divides its data in three segments and with each segment parties add different random number.

Steps:

1. Each party send its sum of first segment D_{11}, D_{21}, D_{13},....D_{n1} and random no. r_{11}, r_{21}, r_{31}.....r_{n1} to third party.
2. (i) Third party do sum of all the first segments received from all the parties P_1, P_2, P_3....P_n i.e. S.
   (ii) Third party send sum S to party P_1.
3. Party P_i subtracts its random no. r_{i1} and add its second segment D_{i2} and its random no. r_{i2} and then send sum to next party P_{i+1}. This step repeat till $i=n$.
4. Party P_n send sum S to P_{n-1}.
5. Party P_{n-1} subtracts its random no. r_{i2} and add its third segment D_{i3} and its random no. r_{i3} and send sum to previous party P_{i-1}. This step repeat till $i=1$
6. Party P_1 send sum S to TP and TP send this sum to P_n.
7. Party P_n subtracts its random no. r_{n2} and add its third segment D_{n3} and send sum to P_{n-1}.
8. Party P_{i-1} subtracts its random no. r_{i3} and send sum to P_{i-2}. Repeat this step till $i=1$.
9. Party P_1 sends sum S to TP.
10. Third party TP broadcast the sum S to P_1, P_2, P_3,….P_n.

V. Architecture for Hybrid technique of secure Sum Computation

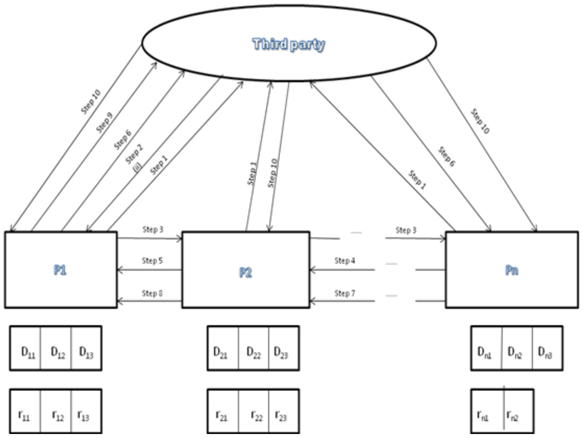

Figure 1: Hybrid Secure Sum Architecture

VI. Formal Description

Sum Protocol Algorithm

1. Assume P_1, P_2, P_3,....P_n are n parties involved in Hybrid secure computation.
2. Each party divides its data D_i in three segments D_{i1}, D_{i2} & D_{i3} and division of data in segments will be decided by parties itself, where $i= 1,2,3…n$.

```
3.  Each party decide three random no. $r_{i1},r_{i2},r_{i3}$ for each segment except nth party. Nth party has only two random nos. $r_{n1}$& $r_{n2}$ for first two segments.
4.  For $i=1$ to $n$
            $S=\sum_{i=1}^{n}(D_{i1}+r_{i1})$
5.  $TP$ send sum $S$ to party $P_1$.
6.  for $i= 1$ to $n$
            $S= [(S-r_{i1})+(D_{i2}+r_{i2})]$
7.  $n^{th}$ party send Sum $S$ to $(n-1)^{th}$ party.
8.  for $i= n-1$ to 1
            $S= [(S-r_{i2})+(D_{i3}+r_{i3})]$
9.  Party $P_1$ send sum $S$ to third Party $TP$.
10. $TP$ send sum $S$ to nth party.
11. for $i= n$ to 1
    Begin
    If $i= n$
    Then
            $S= [(S-r_{i2}) + (D_{i3})]$
    // $S$ is a global variable

    Else
            $S= [(S-r_{i3})]$
12. Party $P_1$ send final Sum $S$ to $TP$.
13. $TP$ broadcast sum $S$ to all the parties.
```

VII. Analysis of Hybrid Technique of secure Sum Computation:

Case I: If any party and third party become malicious.

If any one party and third party collude party can know only data of itself and third party knows the segment of party by whom it colludes. There is no other way of knowing the input data of other parties.

Case II: If any two parties collude:

If any two parties collude they can't get the data of other parties because data is divided into segments and each segment is secure with random number added in each round.

Case III: When all the parties are honest including third party.

When all the parties are honest including third party the protocol did not need so many rounds and addition of random numbers. The sum can be obtain in single round. But it is a ideal condition that's why our protocol has so many rounds and in each round of communication we perform addition and subtraction of random numbers. Due to which communication and computation complexity increases for computation of correct result. This is costly and time consuming protocol.

Computation complexity is

In first round computation at TP= 1
In second round computation on all the parties clockwise i.e. P_1 to $P_n= n$
In third round computation on all the parties anticlockwise i.e. $P_{(n-1)}$ to $P_1= (n-1)$
In fourth round computation on all the parties anticlockwise P_n to $P_1= n$
On adding all the values obtain in each round we get:
$1+n+(n-1)+n= 3n$
$3n$ is the computation complexity of our protocol.

Communication complexity is $(4n+1)$.
The communication and computation complexity of our protocol is $O(n)$.

VIII. Conclusion and Future Scope:

In this paper we suggest a new model for secure sum computation. New model is combination of previous models i.e. ideal model and real model we named it as Hybrid Model. In hybrid model computation of input data of individual parties is computed with the help of parties and third party. Parties and third party both do computation at their end and final result is broadcast by third party to all the parties.

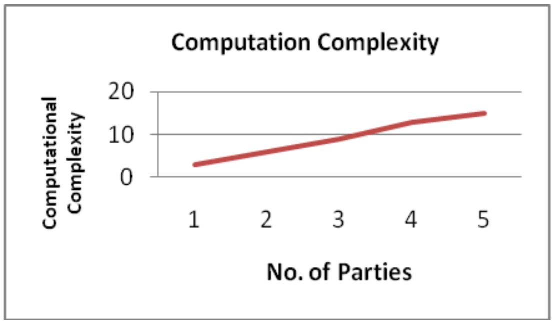

Figure 2: Computational Complexity

Our protocol is completely secure which give zero data leakage. In case any party becomes malicious or two parties collude then too the secure computation is possible without data leakage. Malicious parties cannot identify or calculate the actual data or segment in any round of algorithm; they only get some computed part of data by which no relevant information is retrieved.

Our protocol is complex because of security and privacy constraints due to which computation and communication complexity increases. The computation and communication complexity is $O(n)$.

In future we try to reduce the complexity of our protocol without affecting the security and privacy of input data.

References

[1] A.C.Yao, "protocol for secure computations," in proceedings of the 23rd annual IEEE symposium on foundation of computer science, pages 160-164, Nov.1982.

[2] Y. Lindell, "secure multiparty computation for privacy preserving data mining," IBM, T.J. Watson Research Center, USA, http: // u.cs.biu.ac.il/-lindell/ research-statements / mpc- ppdm.htm/2001

[3] W. Du and M.J. Atallah, "Secure Multiparty Computation Problems and Their Applications: A Review and Open Problems," In proceedings of new security paradigm workshop, Cloudcroft, New Maxico, USA, page 11-20, Sep. 11-13 2001.

[4] O. Goldreich, S. Micali and A. Wigderson, "How to play any mental game." In proceedings of the 19th annual ACM Symposium on Theory of Computation, pages 218-229, May 1987.

[5] Goldreich, "Multiparty Computation (Working Draft)," Available from http: //www.wisdom.weizmann.ac.il/ home / oded / public html / foc.html, 1998.

[6] R. Agrawal and R. Srikant. "Privacy-Preserving Data Mining," In proceedings of the 2000 ACM SIGMOD on management of data, Dallas, TX USA, pages 439-450, May 15-18 2000.

[7] W. Du and M.J. Atallah. "Privacy-Preserving Cooperative Scientific Computations," In 14th IEEE Computer Security Foundations Workshop, Nova Scotia, Canada, pages 273-282, Jun. 11-13 2001.

[8] W. Du and M.J. Atallah, "Protocols for Secure Remote Database Access with Approximate Matching," In 7th ACM Conference on Computer and Communications Security (ACMCCS 2000), The first workshop on security and privacy in e-commerce, Athens, Greece, Nov. 1-4 2000

[9] M. J. Atallah and W. Du. "Secure Multiparty Computational Geometry," In proceedings of Seventh International Workshop on Algorithms and Data Structures(WADS2001). Providence, Rhode Island, USA, Pages 165-179, Aug. 8-10 2001.

[10] W. Du and M.J.Atallah, "Privacy-Preserving Statistical Analysis," In proceedings of the 17th Annual Computer Security ApplicationsConference, New Orleans, Louisiana, USA, pages 102-110, Dec. 10-14 2001.

[11] Clifton, M. Kantarcioglu, J.Vaidya, X. Lin, and M. Y. Zhu, "Tools for Privacy-Preserving Distributed Data Mining,"J. SIGKDD Explorations, Newsletter,vol.4, no.2, ACM Press, pages 28-34, Dec. 2002

[12] D. K. Mishra, N. Koria, N.Kapoor and R.Baheti, "A Secure Multiparty Computation Protocol for Malicious Computation Prevention for Preserving Privacy during Data Mining," International Journal of Computer Science and Information Security, Vol. 3, No. 1, pages 79-85, Jul. 2009.

[13] Durgesh kumar Mishra and Manohar Chandwani, "Zero-hacking Protocol for Secure Multiparty Computation using Multiple TTP", Acropolis Institute of Technology and Science, Inodre, Institute of Engineering and Technology, DAVV University, Khandwa Road Indore, M.P., India, mishra_research@rediffmail.com, mc.iet@dauniv.ac.in.

[14] R. Sheikh, B. Kumar and D. K. Mishra, "Privacy-Preserving k-Secure Sum Protocol," in International Journal of Computer Science and Information Security, vol. 6 no.2, pages 184-188, Nov. 2009.

[15] R. Sheikh, B. Kumar and D. K. Mishra, "Changing Neighbors k- Secure Sum Protocol for Secure Multi-party Computation," Accepted for publication in the International Journal of Computer Science and Information Security, USA, Vol.7 No.1, pp. 239-243, Jan.2010.

[16] R. Sheikh, B. Kumar and D. K. Mishra, "A Distributed k-Secure Sum Protocol for Secure Multi-party Computation," submitted to a journal, 2009.

[17] R. Sheikh, B. Kumar and D. K. Mishra, "A Modified ck-Secure Sum Protocol for Multi-Party Computation," Journal of Computing, USA, Vol. 2, Issue 2, pages 62-66 , Feb. 2010.

AUTHORS PROFILE

Priyanka Jangde

Ms. Priyanka Jangde received her Bachelor of Engineering degree in Information Technology from Samrat Ashok Technological Institute in 2007, Vidisha, M.P.,India. Presently she is pursuing M.Tech. (Information Technology) from SSSIST, Sehore, M.P., India. She has published paper in referred International/National Conferences. She is a member of IEEE.

Gajendra Singh Chandel

Mr. Gajendra Singh Chandel received his Bachelor of Engineering degree in Information Technology from Oriental Institute of Science and Technology, Bhopal, M.P., India. He has completed his M.Tech (Master of Technology) degree in Information Technology from Lakshmi Narain College of Technology, Bhopal, M.P., India. Presently he is Professor in SSSIST, Sehore, M.P., India.

Durgesh Kumar Mishra

Dr. Durgesh Kumar Mishra has received M.Tech. degree in Computer Science from DAVV, Indore in 1994 and PhD degree in Computer Engineering in 2008. Presently he is working as Professor (CSE) and Dean (R&D) in Acropolis Institute of Technology and Research, Indore, MP, India. He is having around 21 Yrs of teaching experience and more than 6 Yrs of research experience. He has completed his research work with Late Dr. M. Chandwani, in Secure Multi- Party Computation for preserving Privacy. He has published more than 75 papers in refereed International/National Journal and Conference including IEEE, ACM etc and listed in DBLP, Citeseer, etc. He is a Senior Member of IEEE and having responsibility of Chairman of IEEE MP subsection and Chairman IEEE Computer Society, Bombay Chapter, India. Dr. Mishra has delivered his tutorials in IEEE International conferences in India as well as in other countries. He is also the program committee member of several International conferences and Member of Editorial Board of National and International refereed Journals. He visited and delivered his invited talk in Taiwan, Bangladesh, Singapore, Nepal, USA, LONDON, UK and several places in India in Secure Multi-Party Computation of Information Security for preserving privacy. He is an author of one book also. He is also the reviewer of four International Journals of Information Security. He is a Chief Editor of Journal of Technology and Engineering Sciences. He has been a consultant to industries and Government organization like Sale tax and Labor Department of Government of Madhya Pradesh, India.