International Journal of Data Engineering (IJDE)
Singaporean Journal of Scientific Research(SJSR)
Vol.7.No.1 2015 Pp.353-358
available at:www.iaaet.org/sjsr
Paper Received :26-12-2014
Paper Accepted:14-01-2015
Paper Reviewed by: 1 Prof. Narayan Chowdry 2. Chai Cheng Yue
Editor : Dr. Chu Lio

ZERO PERCENTAGE DATA LEAKAGE AND HIGH PRIVACY OF DISTRIBUTED R_K SECURE SUM PROTOCOL

Dr.K.Venkatachalapathy
Professor
Department of Computer Science and Engineering
Annamalai University
Annamalai Nagar -608 002.

E. Gokulakannan
[*]Research Scholar/ [**]Assistant Professor
[**]Department of Computer Science and Engineering
[*]Annamalai University / [**]M.R.K Institute of Technology
[*]Annamalai Nagar -608 002./[**]Kattumannarkoil -608301

Abstract: **Secure multi party computation permits many parties to compute some function of their inputs while not revealing the particular input to one another. Secure add computation is simply unwritten paradigm and therefore the element of the various Secure Multi-Party Computation solutions. Secure add computation permits parties to reason add of their individual inputs with no revealing the inputs to one another. This is break the data block of each party into number of data segments and redistribute the data segments among parties before the computation after adding the own random number. These complete steps create circumstances in which it becomes impractical for semi honest parties to know the private data of some other party presents in the bus network architecture. Here all the parties arranged in Bus topology. This protocol is advancements to all the previous protocol because this protocol is used bus topology to calculating the global result without disclosing their result. So the number of complexity of this protocol is decreased with zero percentage of data leakage. During this paper, have a tendency to propose a changed version of Rk-Secure add protocol with extra security once a grouping of the computing parties conspires to know the information of some party.**

Keywords: Privacy, Secure sum, Secure Multi Party computation, Modified Rk Secure sum protocol, Distributed Database Partition

I. INTRODUCTION

The enormous growth of the web and its unexacting access by mortal created opportunities for combined computations by numerous parties. All the collaborating parties for the sake of their joint benefit want to compute the ordinary perform of their inputs, however at the same time they are anxious about the privacy [6][7][8][10] of their information. This subject of the knowledge security is called Secure Multi-Party Computation(MPC). This subject has two goals; one is the privacy of the individual information inputs and another is the correctness of the result. In the main two models are present in the paper for the analysis of the Secure Multi-Party Computation problems. The ideal model of the Secure Multi-Party [11][12][13][14] Computation uses a trusted Third Party aside from the collaborating parties. Parties to supply their inputs to the trusted Third Party Computation of the perform is done by the trusted Third Party then the result's sent to all or any other parties. During this paradigm the trustiness of the trusted Third Party is critically necessary as a result of the trusted Third Party turns corrupt, it will supply the private inputs of one party to others. However it is widely used model of the

Secure Multi-Party Computation due to its straightforward implementation and the protocols available that avoid the trusted Third Party to act cruelly. A real model of the Secure Multi-Party Computation does not use any trusted Third Party however the parties themselves agree on some protocol for the computation. The party performance in the Secure Multi-Party Computation is vital to mirror on authentic party follows the protocol and respects the privacy of different parties. A semi honest party follows the protocol, however also tries to learn different data than the result. The corrupt party neither follows the protocol nor respects the privacy of different parties totally different protocols are needed for dissimilar Secure Multi-Party Computation models and the behaviour of the party. Solutions are available for Secure Multi-Party Computation problems with science techniques, organization techniques and anonymization methods. The subject of Secure Multi-Party Computation has been evolved from two party relationship problems[1] to multi party representation pattern matching problems. Many specific Secure Multi-Party Computation problems have been outlined and analysed by researchers approximating non-public info Retrieval, Selective operate analysis, Privacy-Preserving database query, Privacy-Preserving Geometric Computation, Privacy- protective applied mathematics Analysis, Privacy-Preserving Intrusion Detection and Privacy-Preserving Cooperative Scientific Computation. Based on these general Secure Multi-Party Computation(MPC) problems, many world applications emerged like Privacy-protective Electronic voting, Privacy-Preserving Bidding and Auctions, Privacy-Preserving, Social Network Analysis, Privacy-Preserving Signature and Face Detection, etc. Secure sum computation problem of Secure Multi-Party Computation can be outlined as: however multiple parties can cypher the sum of their input values while not disclosing definite values to at least one another. Secure sum can occupation as to implement for the Secure Multi-Party Computation solutions in the privacy protective spread data mining problems [1][2][3]. In our system have a tendency to proposed a novel Rk-secure sum protocols with additional security just in case a group of the parties joins together and need to understand the non-public knowledge of some other party.

A. *Secure sum*

Secure sum [1][4][5][6] is appropriate only for two parties for providing the security. In this protocol one party send the partial support to the next party with adding their own random number, and then the last party will disclose the result. Many secure sum protocol are available like Yao (1), Ln(x) [2], secure union protocol etc.

B. Secure Multi Party Computation

Secure multi party computation [11][14][15] is applicable when the number of parties more than two. In which one party calculates their partial support and send to the next parties after adding the own random number. Then the last parties will disclose their result.

II. Related Works

The paper [1] studied the problem of secure mining of association rules in horizontally partitioned databases. Tamir Tassa proposed here a protocol Fast Distributed Mining algorithm (FDM) for mining of association rules in horizontally distributed databases. The key idea is that the players finds their locally s-frequent itemsets then the players check each of them to find out globally s-frequent item set. Paper assumes that the players are semi honest; they try to excerpt information. Hence the player compute the encryption of their private database together by applying commutative encryption. The paper shows that their protocol offers better privacy and is significantly more efficient in terms of communication cost and computational cost while the solution is still not flawlessly **secure cause it leaks excess information [1].**

The paper [4] proposed privacy preserving data mining using Extended Distributed Rk Secure Sum protocol in combination with apriori algorithm where firstly mining of frequent items from individual parties is done with apriori algorithm then applied Extended Distributed Rk-secure sum protocol to obtain global result. Apriori Algorithm follows bottom up strategy to find frequent item sets. The distributed RK-secure sum protocol is secure multi party computation protocol, holds frequent itemsets globally without affecting privacy. where the parties p1, p2,...pn are arranged in bus network. p1 is protocol initiator and pn is last party. If two parties join together the network then possibility that they can know each other's data. So to reduce this drawback extended distributed Rk-secure sum protocol is used which is also a secure multi party computation protocol, but this also has some disadvantages over another techniques.

Like paper [4], the paper [5] also uses apriori algorithm for generating association rules and playfair cipher technique is used to transfer that generated rules. This paper defines two parts of association rule; Antecedent, is the item found in database and consequent, found in combination with the first. Unlike all cipher technique, playfair cipher encrypts pair of letters. This technique uses a 5 by 5 table containing a keyword. firstly, table have to fill up with keyword and remaining spaces with remaining spaces removing the duplicate letters. I and J are written in one column encrypts pair of letters.

In this paper [6], association rules are generated and global frequent item sets in distributed environment if originate with the help of FP tree. FP tree is a compact data structure. It finds frequent item set lacking of generating candidate item set by traversing frequent item set through FP tree. This paper also provide privacy to the databases with Data Encryption Standard(DES). In DES two keys are used, first party encrypts dataset with key 1

and this encrypted data is again encrypted with key 2. The receiving party decrypts data with key2 first then key1. This is also called as Double Encryption and it provides higher security to databases than other cryptographic technique. This paper shows that global frequent item set is found with negligible communication and time complexity with zero percentage of data leakage. But **this is only applicable for homogeneous databases.**

The paper[7] deals with the problems of association rule mining. The problems can be divided as data hiding and knowledge hiding. Data hiding is defined as the trial of removing confidential or private information from the data before its disclosure. Knowledge hiding, on the other hand, concerns the information ,or else the knowledge, that a data mining method may discover after having analyzed the data. This paper reviews the methods of privacy preserving and proposed an improvement of sensitive rule hiding to make it more accurate and secured. The secure multiparty computation(SMC) is used to find global support and confidence without data leakage. To provide privacy to the database Tiny Encryption Algorithm (TEA) is used.

III. BACKGROUND WORK

The secure multi-party computation started once the two millionaire's party needs the results of one another without disclosing the individual result. The thought of two parties [1] are going to be extended [6] when they are exploitation the secure total and secure multi party computation. It is one in each of the security protocols employed in classification for conserving privacy of censored information to provide extra security and preserve individual information, this protocol was modified in [2].

Let us contemplate a scenario where over two parties (say n) want to cipher and use classification technique during a secured approach. So, according to the protocol [2][14][15], first party adds a random number to its value and sends the result to second party. Second party adds its result to the other result and sends to the third party. This method continues till the last party (n) receives the result from the previous party (n-1). This party adds its result and sends the output to next party. Secure multi party computation has two main goals one is provides the security to individual information and another is correctness of result. Yet as secure multi party computation contains two main models one is real model and another is ideal model. In real model there is no any trusty party, but in ideal model there is trusty party is present. The full secure multi party computation divides into three components according to their inputs. The first one is convert the inputs into secure multi party computation. When the computation and the second one is converting the inputs into homogeneous secure computation and another is converting the inputs into heterogeneous secure computations [8][9][11]. Figure 1 shows the secure multi party computation.

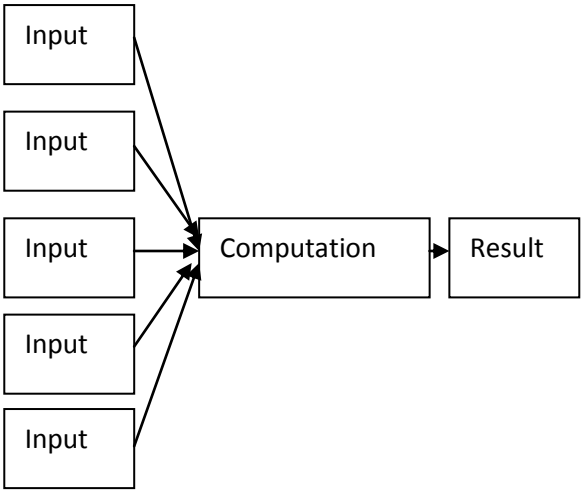

Figure 1: Diagram of Secure Multi Party Computation

IV. PROPOSED WORK

When the concept come of distributed database [8][12][13] in which the whole database is divided into the number of parties and each party want that their own result will not known by the other parties. So concept of security and privacy play an important role. Here it is proposed modified and updated version of Rk Secure Sum protocol for providing the highest privacy and zero percentage data leakages to the distributed database. In this proposed and novel protocol, all the parties are arranged in a sequential manner and party P1 is considered as a protocol initiator party. If there are N numbers of parties, then number of round is also ' n'. But the condition is that party P1 will always change their position in each round till the party Pn. After that P1 will disclose the result. First the P1 calculate their own partial support and added their own random number and send to the next party till Pn. After the completion of n^{th} round party P1 will disclose the global result that accepted by all the parties presents in the distributed database. The Algorithm shows formal working steps of modified R_k secure sum protocol. Figure 1 shows the number of rounds from 1, 2, 3, 4, 5 and 6.

Algorithm of Modified Rk Secure sum Protocol
Step1:- Select N number of parties from P1, P2,P3,P4…Pn. (n≥5).
Step2:- Consider each party has a random number R1, R2,R3,R4……..Rn.
Step3:- Each parties (P1, P2, P3, P4…Pn) have their data D1, D2, D3, D4……..Dn.
Step4:- Arranged the parties in a bus structure(P1, P2, P3, P4…….Pn) and select P1 is protocol initiator.
Step5:- Assume RC=n and Pij=0 /*RC is round counter and Pij is partial support */
Partial support will calculate using the following formula Pi=P (i-1) +RC
Step6:- While RC! =0

Begin
Begin
For 1 to n do
Begin
Starting from P1 each party will compute their partial support and send to the next
party in the bus
End
P2 exchange its position to the next party present in the bus till Pn.
End
RC=RC-1
Step7:- Party P2 will announce the result after calculating from all the parties.
Step8:- End of algorithm

- Number of rounds in Modified Distributed R_K secure sum Protocol is lesser as compared to the existing one because in a single round that not required to n number of data segment round again.

- The complexity of the Modified Distributed R_K secure sum Protocol is also reduced as compared to the existing one because the segmentation of data is not required in the proposed one.

VI. Performance Analysis

In this Modified Distributed R_K secure sum Protocol the number of parties is N and the number of rounds is (N- 1) because each party will exchange its position to the next party presents in the bus network. The only one limitation of this bus topology is that each rounds exchange its position. The computation and communication complexity both come to N. Thus we can write the communication complexity C(n) and computation complexity S(n) are shown in figure 2.

C (N) =N
S (N) =N

The communication and computation complexity both come in order of N

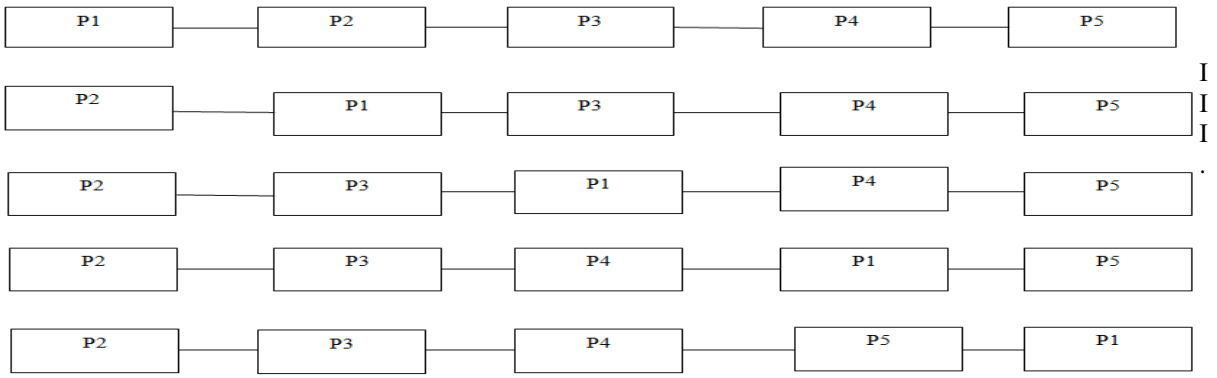

Figure 2: Shows the Process of each round (1, 2, 3, 4, 5,6)

V. Comparison between the Existing One and Modified Distributed RK secure sum Protocol

- Existing one approach is using the Ring topology [9][10][11] but the Modified Distributed R_K secure sum Protocol is using the bus topology so that it's easy to design the bus architecture as compared to ring architecture because in bus the all parties are connected in a serial manner.

- In existing one the segmentation of data is occurred for each party, but in the Modified Distributed R_K secure sum Protocol the segmentation of data is not necessary, because of segmentation of data is done then required the highest privacy as compare to transfer blocks of data at once.

- In block of data not required as much of privacy and it's more secure as compare of segments of data.

VII. CONCLUSION

Secure protocol is an important construction of secure multi party computation. The secure multi party computation within which the probability of data outflow is Zero. In this proposed protocol give a zero percentage of data leakage is zero. When two or more parties want to understand the information for alternative nearer party. In this modified and updated Rk Secured protocol knowledge is transferred within the kind of blocks. In order that the privacy required in this protocol is extremely less as compared to the phase of data transmission. The complexity of this new protocol is O(N). In future it will implement a protocol that have complexity, but O(N) and co-jointly give the highest privacy to the distributed database. In this paper Modified Distributed R_k secure add Protocol provides a zero probability of data outflow by two or more colluding parties which want to understand the information of some

party. In this Distributed R_k secure add Protocol, the information block of every party is broken into a precise number of segments and computation is performed over these segments. The parties extent unit allowed to vary their position within the bus topology. This ensures that a party cannot have the same neighbors for all the rounds of the computation. Thus, two or more conspiring parties cannot learn the key knowledge of some other party. This is an improvement over previous protocols which guarantee and safety for colluding neighbors solely. Further efforts will be done to style and analyze the protocol for malicious parties neither follow the protocol nor honor the privacy of the parties. Protocols will be designed to make the information secure just in case majority of the parties extent unit is also semi honest. Here all the parties arranged in Bus topology. This protocol is advancements to all the previous protocol because this protocol is used bus topology to calculating the global result without disclosing their result. So the number of complexity of this protocol is decreased with zero percentage of data leakage. During this study, have a propensity to propose a changed version of Rk-Secure add protocol with extra security once a grouping of the computing parties conspires to know the information of some other party.

REFERENCES

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

[2]. Tamir Tassa,"Secure mining of association rule in horizontally distributed databases" ,IEEE trans. Knowledge and Data Engg. ,Vol. 26, no.2, April 2014.

[3]. M. Kantarcioglu and C. Clifton, "Privacy-Preserving Distributed Mining of Association Rules on Horizontally Partitioned Data," IEEE Trans. Knowledge and Data Eng., vol. 16, no. 9, pp. 1026-1037, Sept. 2004.

[4]. Krishna Pratap Rao, Adesh chaudhary, Prashant johri "Elliptic Curve Cryptography Based Algorithm for Privacy Preserving in Data Mining", International Journal for research in Applied Science and Engineering Technology (IJRASET) ,Vol. 2 Issue V, May 2014.

[5]. Meera Treesa Mathews, Manju E.V," Extended Distributed R_KSecure Sum Protocol in Apriori Algorithm for Privacy Preserving", International Journal of Engineering and Advanced Technology (IJEAT), Volume-3, Issue-4, April 2014.

[6]. P. Jagannadha Varma, Amruthaseshadri,.M. Priyanka, M.Ajay Kumar, B.L.Bharadwaj Varma, " Association Rule Mining with Security Based on Playfair Cipher Technique" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5, 2014.

[7]. Jyotirmayee Rautaray, Raghvendra Kumar, "Privacy Preserving In Distributed Database Using Data Encryption Standard (DES) ", International Journal of Innovative Research in Science, Engineering and Technology Vol. 2, Issue 3, March 2013.

[8]. Prof. Geetika. Narang, Anjum Shaikh, Arti Sonawane, Kanchan Shegar, Madhuri Andhale," Preservation Of Privacy In Mining Using Association Rule Technique", International Journal of Scientific & Technology Research, Volume 2, Issue 3, March 2013.

[9]. C. 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, pp. 28-34, Dec. 2002.

[10]. 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.

[11]. R. Sheikh, B. Kumar and D. K. Mishra, "Privacy-Preserving k- Secure Sum Protocol," in the International Journal of Computer Science and Information Security, USA, Vol. 6 No.2, pp. 184-188., Nov. 2009.

[12]. R. Sheikh, B. Kumar and D. K. Mishra, "A Distributed k-Secure Sum Protocol for Secure Multi-party Computation," submitted to a journal, 2009. [6] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game," in STOC '87: Proceedings of the nineteenth annual ACM conference on Theory of computing, New York, NY, USA, ACM, pp. 218-229, 1987.

[13]. B.Chor and N.Gilbao. "Computationally Private Information Retrieval (Extended Abstract)," In proceedings of 29th annual ACM Symposium on Theory of Computing, El Paso, TX USA, May 1997.

[14]. B. Chor, E. Kushilevitz, O. Goldreich,and M. Sudan, "Private Information Retrieval ," In proceedings of the 36th Annual IEEE Symposium on Foundations of Computer Science, Milwaukee WI, pp. 41-50, Oct. 1995.

[15]. Y. Lindell and b. Pinkas, "Privacy preserving data mining," in advances in cryptography-Crypto2000, lecture notes in computer science, Vol.1880, 2000.

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

[17]. 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, pp. 165-179, Aug. 8-10, 2001.

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

[19]. W. Du and M.J.Atallah, "Privacy-Preserving Statistical Analysis, "In proceedings of the 17th

Annual Computer Security Applications Conference, New Orleans, Louisiana, USA, pp. 102-110, Dec. 10-14 2001.

[20]. 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, pp. 11-20, Sep. 11-13, 2001.