ISSN:0975-9646

Analysis of Data and Traffic Management during Privacy Preservation in Secure Multiparty Computation

Zulfa Shaikh[#1], Tonu Sojatia*[2], Mrs Pushpa Pathak[#3], Mrs Shilpa Bhalerao*[4]
[#]Master of Computer Application
Acropolis Institute of Technology and Research
Indore,M.P.,India
[1]shaikh.zulfa@gmail.com
[3]pushpathak2007@rediffmail.com
*Deptt of Information Technology
Acropolis Institute of Technology and Research
Indore,M.P.,India
Master of Computer Application
Acropolis Institute of Technology and Research
Indore,M.P.,India
[2]tonusojatia@gmail.com
[4]hodfca@acropolis.in

***Abstract*-A protocol is secure if the parties who want to compute their inputs hands it to the trusted parties. Trusted parties in turn compute the inputs using the function f and give the result to the respective parties after computation in such a way that no party can identify other's party data. During computation of inputs, we had considered the factor, what if trusted third parties are malicious? Considering different probabilities for the malicious users, we have tried to find out the correctness of the result and percentage of system acceptability. We then tried to increase the number of TTP's in order to get the accuracy of the result. The aim of our proposed work is to identify what probability of malicious users will lead to the system in an unacceptable state.**

In this paper, we also propose the methodology and design an algorithm to control congestion during Secure Multiparty Computation (SMC). As per our literature serve a lot of work has been done in SMC but they have worked only the main part of the SMC, privacy and correctness. Congestion control is one of the important components for the performance of the network and also is the most challenging one. In our previous research we assumed that the communication between party and a nonymizer is secure, but if any anonymizer becomes malicious then entire data of one party can be hacked. In this protocol, to maintain the security between party and anonymizer we have partitioned the data in number of packets before sending to a nonymizer. We propose the framework in the form of a protocol for secure multi-party computation. This protocol maintains the security when we transfer the data between party and anonymizer. This paper deals with the way of shaping the traffic to improve quality of service (QoS) in SMC. Since on increasing the number of packets there may be a problem of congestion and under the congestion situation, the queue length may become very large in a short time, resulting in buffer overflow and packet loss. So congestion control is necessary to ensure that users get the negotiated QoS. The objectives of traffic control and congestion control for SMC are: Support a set of QoS parameters and minimize network and end-system complexity while maximizing network utilization.

In our paper we also carried out experiments for computing the FIFO length that ensures zero packet loss for different clock rate of the router.

***Keywords*- Security, Probability, Trusted Third Party, System acceptability, Congestion, Quality of Service, Secure Multiparty Computation.**

I. INTRODUCTION

Formally, we can define SMC problem as a situation where there are n parties having private inputs *x1, x2, x3…….,xn* respectively and they want to compute the value of the public function y=*f*(x1,x2,……..,xn) such that after the completion of computation no party has any information about the inputs of other parties apart from the information

revealed by the computed result [1]. For the computation, we make use of a trusted third party to do the computation on the inputs provided by the parties. According to [2], the major problem with this approach is that it is difficult to find the third party which is trusted by all the parties providing the inputs.

In this paper, we have tried to find out the probability up to which we can find the correctness in the result when the computation is being done by the third parties assuming that the trusted third parties are malicious.

The proposed work here is to identify the correctness of the result on different probabilities of malicious users. We had also identified the probability after which the system acceptability fails. We also tried to get more accurate result on increasing the number of TTP's and arrived at some conclusion which is being depicted by the graph analysis. We also carried out experiments for computing the FIFO length that ensures zero packet loss for different clock rate of the router.

I. RELATED WORK

SMC problem is the problem of n parties to compute a private function of their inputs in a secure method, where security means the correct result computed by the TTP's for maintaining the privacy of the parties as some of the parties may want to misuse the other party's data.We assume that we have inputs *x1,x2,…xn* where xi is the data of party Pi and the TTP will compute a function f(x1,x2,….xn)=(y1,y2,….yn) and sends the result to the respective parties so that party Pi will receive only yi and not the result of other parties for the security purpose. Security is meant to achieve correctness of the result of computation and keeping the party's input private even if some of the parties are corrupted.

Yao's introduced the SMC problem in [3].His first solution uses a centralized TTP which is selected by majority of honest party, which shows synchronous system with cryptography [4].After handing up the inputs to a trusted third party, security increases but there is a chance that the trusted third party behaves like a malicious adversary. It was demonstrated analytically as well as
experimentally, the performance characteristics and security and proved that for the range of numbers, Yao's protocol is secure[5].

In this paper we have considered the different probabilities of malicious TTP's for which we can get the correct results when inputs are computed by the TTP's and determined the probability of malicious TTP's from where our system starts failing. We have also carried out experiments for computing the FIFO length that ensures zero packet loss for different clock rate of the router.

Our assumption is using anonymizer so that the party can hide identity of its own. To resolve this situation, we make following assumptions.

1. TTP computes the result of the function y=f(*x1, x2… xn*) correctly.

2. TTP has the ability to announce the result of the computation publicly.

3. Each party having the input can communicate with a trusted anonymizer. A trusted anonymizer (*Ai*) is a system that acts as an intermediately between the party having the input and the TTP which will carry out the computation. Thus, *Ai* hides the identity of *Pi* (Party) from the TTP.

4. The communication channels used by the input providing parties to communicate with the anonymizers are secure. That is no intruder that can cut off the data transferred between them.

5. The anonymizer in any condition will not disclose the identity of the data source, from which it is forwarding the data to the third party.

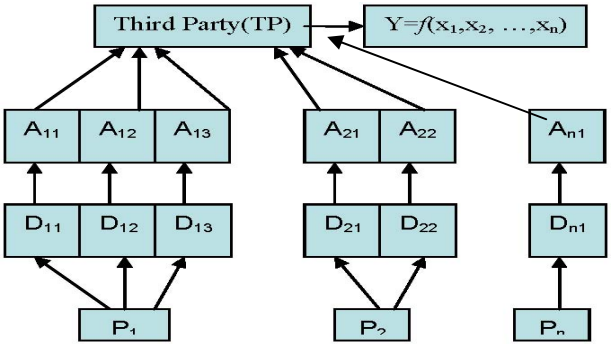

Fig 1.SMC architecture

The concept of breaking the data into number of packets is to increase the security of information. When number of packets increases then the probability of hacking of data will tends to zero so the privacy of party is being achieved which was our previous work.

Our protocol is based on three layers namely computation layer, security layer and input layer. In Figure 1, there are *n* parties *P1, P2…Pn,* each having input *xi* that

will be used in computing y=f(*x1, x2… xn*). To calculate the value of, the each input providing party Pi takes the following steps if the form of an algorithm.

Algorithm for Traffic Management

1. Define P1, P2… Pn. as parties;
2. Define A1, A2… An anonymizers;
3. Generate a random key, Ri, as an identifier for each Pi;
4. Compute di=xi||Ri;

(One method of doing so is to simply append Ri to the data xi)

5. Pi. □.□Ai (A1, A2… An);

/* Pi selects an anonymizer Ai through which Pi will communicate with the UTP. □is the function which select Ai from the A1, A2… An */

6. Send di to Ai; /*Anonymizer receives the appended data from Pi.*/
7. Ai send di to Third Party through some network.
8. As each single packets is divided into number of packets as di1,di2,…din and if input generation rate is higher than the output rate then there may be congestion in the network which may cause packet loss and delay in the network.
9. One way of preventing packet loss is to increase the FIFO length of the router or by increasing its clock rate.
10. Simulations were carried out for message with packet length of 3500.
11. The clock rate of router is varied from 5 Mbps to 100 Mbps.
12. On increasing the clock rate of router, service time of packets at the router and FIFO length required for buffering the packets get reduced.
13. Router then forward the packets to UTP; /*The UTP takes each data unit di and extract xi and Ri from it.*/ End of *Algo*

Fig 2 shows a network connection where each party on different LAN's send packets to the router. Router has forwarding capability which allows it to forward the packet to final destination. On splitting the packet of each party into different number of small packets may lead to a heavy traffic in the network and if the processing rate of the router is less than that of input generation rate then this situation will lead to congestion and finally may result in packet loss. Our study is basically based on how to prevent packet loss in the network.

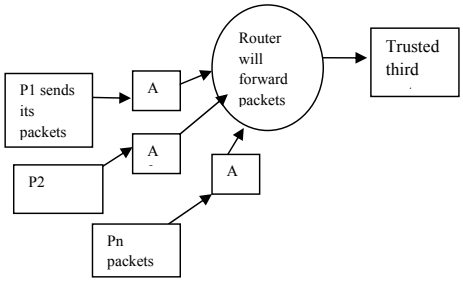

Fig 2.Proposed Network Connection in SMC

III. IMPLEMENTATION OF PROPOSED WORK

A. The first parameter that we had considered during our study is the effect of increasing the probability of malicious users at fixed number of TTP's =1000 and determined the percentage of system acceptability.

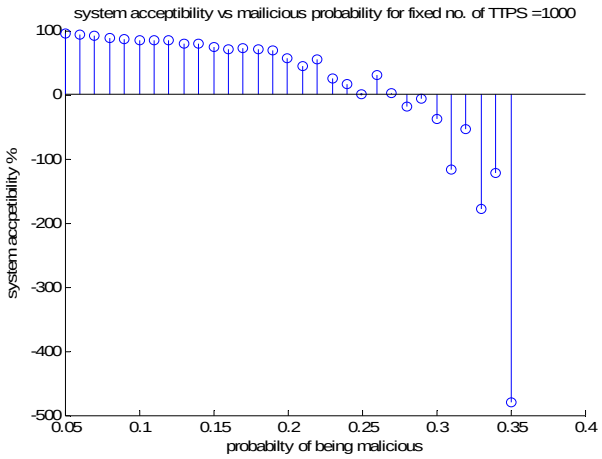

Fig. 3. System acceptability vs. Malicious Probability for fixed no of TTP's=1000

From the graph we concluded that as we increase the probability of malicious users, the system acceptability decreases. And when the probability of being malicious crosses P=0.3 then there is a rapid failure in the system.

B. Then we tested the system acceptability on fixed number of TTP's=5000 and 10000.

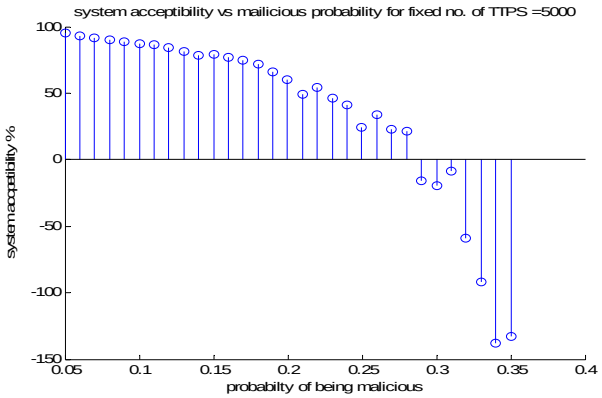

Fig. 4. System acceptability when TTP's=5000

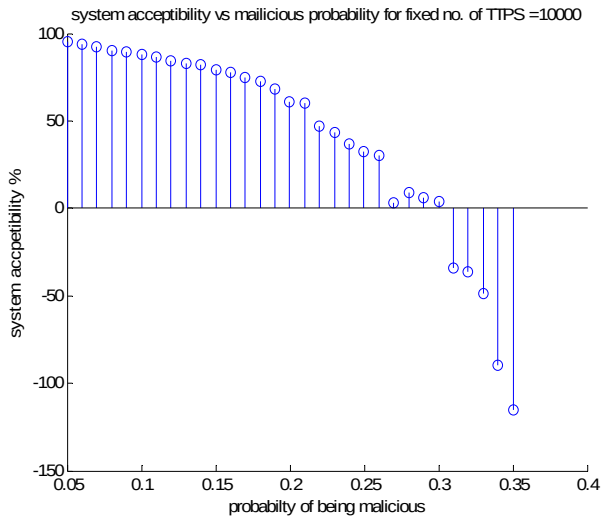

Fig.5. System acceptability when TTP's=10000

Here we arrived at a conclusion that even if on increasing the number of TTP's the system acceptability fails after P=0.3.This means that after P=0.3 the correctness in the result cannot be found.

C. The next parameter that we had considered is varying the number of TTP's on fixed probability of malicious users.

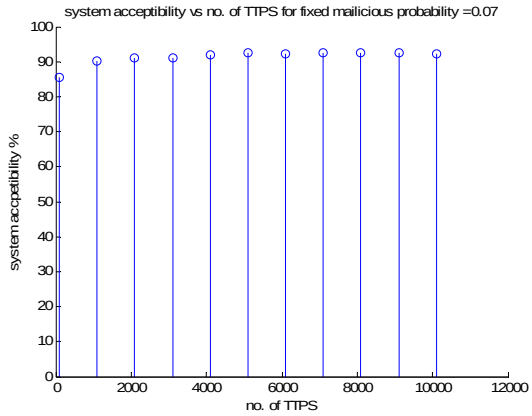

Fig.6. System acceptability vs no of TTP's for fixed malicious probability

Here we arrived at the conclusion that increasing the number of TTP's will not have any effect on accuracy of the result.

D. We also considered the fact that the difference in the packet generation rate at the source and processing rate at the router is the cause of packet loss. Zero packet loss can be ensured if this difference is zero.

The router's processing rate at any time depends on the packet traffic [6, 7]. The traffic at the router varies with time and it is not possible to keep the processing rate of the router same as that of the source. When the traffic is high the packet service time at the router increases which tends to packet loss. In such cases packet loss can be prevented by increasing the FIFO length of the router or by increasing its clock rate. We carried out experiments for computing the FIFO length that ensures zero packet loss for different clock rate of the router. Simulations were carried out for message with packet length of 3500. The clock rate of router is varied from 5 Mbps to 100 Mbps. Higher clock rate reduces the service time of packets at the router and the FIFO length required for buffering the packets also reduces.

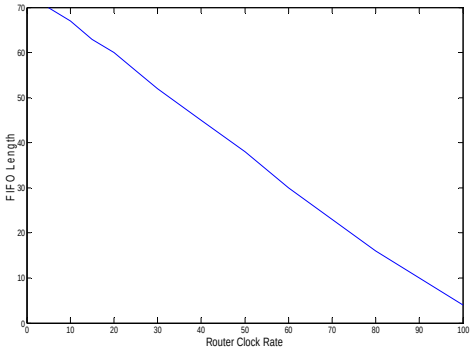

Fig.7. Routers clock rate versus FIFO Length

IV. RESULTS AND CONCLUSION

The result of our study is:-

4.1. The system will be in an unacceptable state after the probability of being Malicious=0.3.
4.2. We conclude that there will be no affect on accuracy of the result on increasing the number of TTP's if the probability of malicious user is fixed.
4.3. Our study concludes that on increasing the clock rate of router, service time of packets at the router and FIFO length required for buffering the packets get reduced which ensures zero packet loss in the network.

REFERENCES

[1] Chris Clifton ,Murat Kantarcioglu, Jaideep Vaidya, Xiadong Lin and Michael Y, "Tools for privacy preserving distributed data mining," SIGKDD Explorations Volume – 4,Issue – 2, 2002,pp. 1-8.

[2] J. Vaidya, and Chris Califton, "Leveraging the Multi in Secure Multi-Party Computation" In the proceeding of the 2003 ACM workshop on privacy in electronic society, ACM Press , October 2003.

[3] A.C.Yao. "Protocol for secure comutations," In Proc. 23rd IEEE Symposium on the Foundation of Computer Science(FOCS), IEEE 1982, pp. 160-164.

[4] O.Goldreich, S. Micali, A Wigderson, "How to play any mental game- a complete theorem for protocol with honest majority." In the proceeding of 19th *ACM symposium on the theory of computing(STOC), 1987,* pp. 218-229.

[5] Ioannidis I and Grama A, "An efficient protocol for Yao's Millionaires Problem," In the Proceeding of *36th Hawaii International Conference on System Sciences,HICSS'03,* 6-9 Jan 2003,IEEE Press, pp. 6-11.

[6] Amir Atai and Joseph Hui "A Rate-Based Feedback Traffic Controller for Networks" Proceedings of the 1994 IEEE International Conference on Communications Vol 3, 1994.

[7] Sanchez, Pedro-Ivan; Mazumdar, Ravi "Definition of congestion: applications to bandwidth management" Proceedings - IEEE INFOCOM Vol 2, 1994.