International Journal of Engineering & Technology, *7 (2.7) (2018) 363-366*

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

A critical review on application of secure multi party computation protocols in cloud environment

A. Vijaya Kumar [1] *, L. S. S. Reddy [2]

[1] *Research Scholar, Assistant Professor, Department of Computer Science & Engineering*
[2] *Professor, Department of Computer Science & Engineering Koneru Lakshmaiah Education Foundation,*
Vaddeswaram, Guntur Dt, Andhra Pradesh, India
**Corresponding author E-mail: vijay.adury@gmail.com*

Abstract

Security is the essential entity of the digital computations in the internet world. Many internet and mobile applications require private data inputs from different clients for data analysis. Now a days many of the Mobile Apps collect the sensitive user data for analysis may be without knowledge of users. Secure Multi Party computation enables distributed users to share their private inputs to a third party which computes a common function over these inputs and the collaborative outcome shared to the user. It is very essential in many engineering, medical and financial sectors where privacy of the sensitive data provided by the user. Many medical researchers require sensitive patient's data for typical diagnosis. This paper detailed the origin for SMC which is secret sharing. It discussed the evolution of two party computation to secure multiparty computation. Several protocols and their pros and limitations are described. Cloud computing changed the way SMC was interpreted by earlier works. Cloud provides all the computations as a service basis is used to drastically reducing the communications overhead of the SMC. Our contribution is focused on evolution from conventional SMC with towards Secure Multiple Computation in collaboration with the cloud. The works focuses on the research issues to be addressed because of the untrustworthy nature of the cloud. A comparative analysis of different approach of SMC is presented. The comparative study details the open issues like transparency, public data auditability in SMC with cloud architecture.

Keywords: *Secure Multiparty Computation; Cloud Computing; Privacy; Transparency; Security; SMC; TTP.*

1. Introduction

The exponential growth of internet and mobile devices generated opportunities for collaborative data analysis among multiple parties where the parties may not trust each other. Hence all the parties want to compute the common function from their secret input values. Secure multiparty computation [1] [2] is meant for these situations. Now a days it is immensely used in privacy preserved data mining [8] SMC has two prime responsibilities: first is privacy of user inputs i.e. no user may not share their input/private data to be shared with other parties, second is the correctness of the data i.e. the value evaluated by the function should be correct and has to be shared only with the participating parties. The Ideal model is make use of trusted third party (TTP) [5]. The trustworthiness of the TTP is important in two aspects. First it should compute the outcome correctly from the inputs received. Second is it should not share the computed outcome with any outside parties or adversaries. There are many models proposed by researchers with TTP using circuit techniques, cryptographic techniques, and randomization techniques. In this paper we discussed the evolution of SMC and how Cloud architecture [3] can be collaborated with the SMC. We also presented the comparative analysis of various approaches on SMC on the parameters. In section 2 basic concepts SMC and cloud are overviewed, in section 3 literature review of evolution of Conventional SMC to SMC collaborated cloud architecture discussed. In section 4 the related work in the distributed model discussed and the comparative analysis is presented which reveals the research gap in the given area. Section 5 summarizes the paper and discuss the future scope in the relative area.

2. Background

Secure Multiparty Computation [1] [2] aims to provide security for multiple parties who want to exchange their private information to compute a public function. If $a_{1,}\ a_{2,\ldots\ldots}\ a_n$ are the private inputs shared by the parties and f be the public function computed as $r=f(a_{1,}\ a_{2,\ldots\ldots}\ a_n)$ in such a way that no party will be knowing the private input shared by the other parties[1] and result r will be shared between all the parties. The term first coined by Yao Ming [1] while explaining the "millionaire problem" in 1982. The computation normally computed within a trusted third party (TTP). All the parties will send their private input data to the TTP and the public function f will be performed in the TTP and the result will be shared across all the parties. The recent years have seen resurrection in evolution [5] [6] [7] [9] of SMC as it is addressing lot many security issues in distributed computing. Many large scale applications are composed of limited number of nodes and resources. This leads to the need for the cloud computing use in executing the computations of secure multi-party computations.
Cloud computing [3] is the latest advancement of IT world which provide services to individuals and organizations who makes use of its services in various forms viz., Software as a Service, Platform as a Service and Infrastructure as a Service. It provides services over the network i.e. Internet. It is possible for the individual user or organizations to access the services of the cloud with few clicks

through Internet. The major advantage of cloud is that users need not look after the maintenance and resource availability. Lot of concerns over the data shared to the cloud platforms. The adaption to cloud computing has lot of concerns because of the security and privacy challenges discussed in [17]. Different approaches have been proposed to overcome these issues [17]. One useful scenario is to transmit the encrypted data to the cloud to prevent the misuse of it. The data to be supplied to the cloud can also be divided into different parts and will be used by a secure function to evaluate the common values from the individual values is another approach towards security ensured cloud computing.

3. Preliminaries

3.1. Secret sharing scheme (SSS)

The basis for Secure Multi party computation is secret sharing scheme [10]. Secret sharing deliver two primary responsibilities share and reconstruct. The reconstruct operation is also referred as open. Share phase takes an encrypted text as input and divide it into number of pieces so that the independent chunks of encrypted information is of no use to any intruder. The reconstruct phase will do the reverse operation. It was independently proposed by Adi Shamir [10] and George Blakley. The primary goal of the scheme is to hide secret information into different chunks.

It the secret word is divided into two shares x, y then the reconstruct preliminary will be as follows

x + y = reconstruct ([x] + [y])

If dot (.) marks sharing and x,y are the two secrets then

x. y = reconstruct (x. [y])

There are different sharing schemes available Shamir [10], Additive sharing in all the shares should reconstruct the original secret, replicated sharing scheme depends on additive sharing but the shares are unqualified subsets. Pseudo random secret sharing (PRSS) [22] is based on RSS generates secret shares which can be converted to Shamir's. Psuedo random integer sharing which is a variant of PRSS which works with integers.

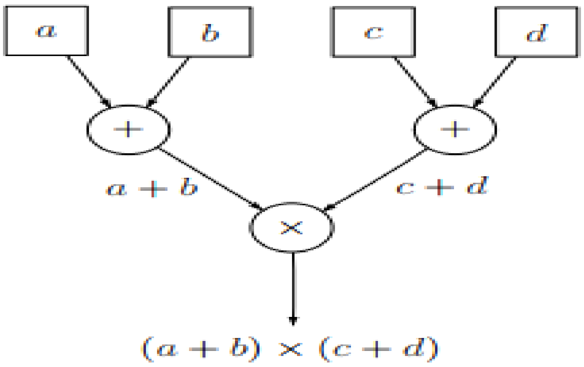

Fig. 1: A Simple Arithmetic Circuit.

3.2. Secure multiparty computation

Secure Multi party computation (SMC) also referred as Multiparty Computation (MPC) was initially discussed by Yao as two-party computation [1]. Two millionaires want to know who is rich between them, but not revealing how wealthy they are to each other. The computation here performed in Semi honest adversary [23] i.e. the third party where computation will be performed is honest in nature and trusted by both the parties.

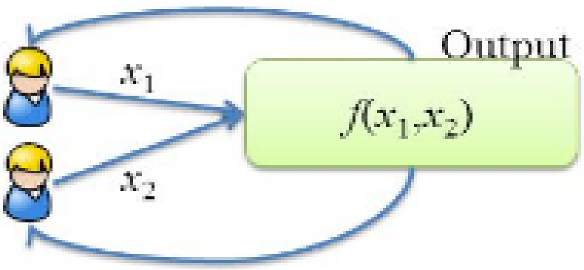

Fig. 2: Yao's Two Millionaires Problem.

Goldreich et al [2] have extended the two party computation proposed to multi-party computation where more than two participate in providing secret information for computing a secret function on the encrypted data submitted by them.

SMC is based on secret sharing [10] in which the data is maintained in privacy preserving [7] manner and distributed across different parties. These data atoms then processed in various modes by applying bitwise AND operations. The computation model typically constructed with Boolean circuits which require oblivious transfer (OT) protocol [20]. Initially several advancement to Yao's Garbled circuits are proposed in implementing SMC. An alternative approach is proposed by Goldreich [2] et al called GMW circuits. Many recent advancements indicate that these protocols are efficient over the Yao's secret sharing protocols.

The SMC architecture has been divided into two ways with respect to the computation performing location. Centralized approach, Distributed approach. In Centralized approach the Parties will submit their secret part information to a Third Party (TP) [5]. The TP will compute the function and share the output to all the parties. The Third party will be a Trusted one, and Untrusted (in real world scenarios).

Trusted third party (TTP): The information received by TTP will not be shared to any adversaries. It's an Ideal situation in real world. It is next to impossible to Trust any Third party to which sensitive information submitted. This is open area to researchers to deal with.

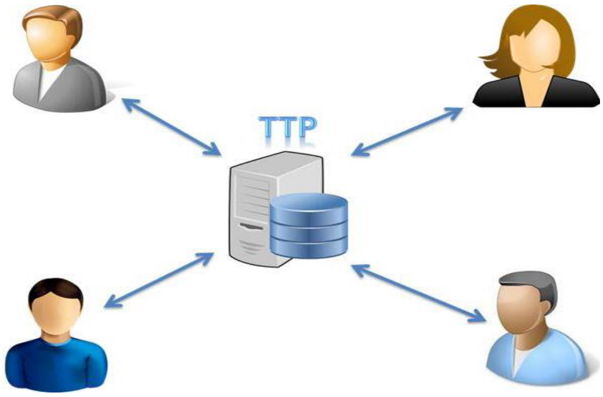

Fig. 3: Multiple Parties Communicating with Trusted Third Party.

The SMC resurrected in recent years with the evolution of the cloud computing. In the distributed SMC approach the computing will be performed in the different distributed nodes collectively compute a same function.

SMC is divided into two groups with respect to the computation ability. 1. Computationally Secure Multi party computation. 2. Information theoretically Secure Multi party computation.

The former is focused on yet to be proved cryptographic primitives which take assumptions which are computationally infeasible, in later approach security is provided unconditionally in this approach although the adversary has large computing ability.

Even though the SMC has lot many advantages it still suffers with the behavior of its corrupt parties which are also called as adversaries. The corrupt parties also called as players and sent of players participating in a computation is referred as a group. Corrupt players [23] in a SMC group are divided into two categories, Passive adversary and active adversary.

A single/set of participants which involve in adversary activities which follow the protocol like normal participants but share the collaborative information gathered in the group which is the violation of the goal of privacy of other players referred as Passive adversary. Active adversary is a single/set of participants which involve directly in adversary activities i.e. violating the protocol information so that the computation results incorrect results and/or violate the privacy of the other players.

3.3. Cloud computing

Cloud computing [3] open doors for small and medium scale organizations to perform computations at very low costs. Cloud consists of several nodes distributed across different geographic locations to provide services to the users as ‘utility based’ services. It outsources Software, Infrastructure and Platforms as Services [24] to its clients. World’s top IT industries like Amazon, Google have set up the large cloud infrastructure already. Although the services provided by the cloud are good, security is the primary theme to be addressed. In a nut shell the primary concern over computations performed in cloud is the privacy. The users outsource the services to the cloud always fear about their data secrecy.

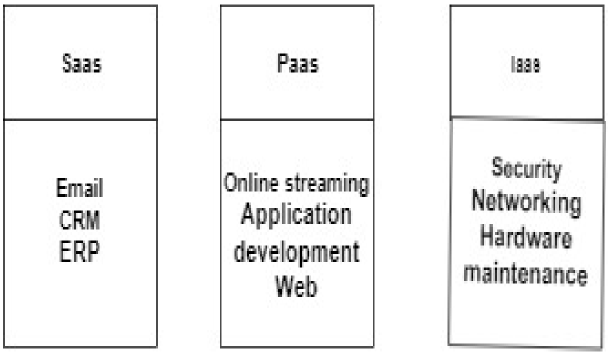

Fig. 4: Cloud Offering Services.

Security: The Key research concern in cloud

The Right scale 2017 state of the cloud report [25] reveals that after lack of expertise in cloud, the cloud security is the most concerned area to address. 25 percent weightage is given alone for security issues in cloud. However for beginners most cited challenge is security with 32 percent concern. Key security issues in the cloud are vulnerability of the data to the third party, data removal from the cloud will not guarantee that the data will be permanently removed from the cloud as redundant copies of data will be maintained in the cloud. No auditability to the data owner as the cloud infrastructure is not in the scope to manage with. Integrity of the data as the data may be modified without the notice of the owner.

4. Related work

SMC is popular for its secret computing capability however the number of data transformations between different nodes make delays in the communications. The Cloud enables to reduce the high interconnectivity delays. Two party SMC was developed with electronic circuits and later extended by Goldreich Circuits. The second circuit approach is more efficient than the two party implementation. SMC can be implemented in several ways: circuit-based approach, Fairplay and FairplayMP [18] are available. Representative based approach SEPIA [20] and Share mind [19]. Next generation of SMCs are developed with Cryptographic algorithms RSA and Parlier. Elliptic Curve cryptography is also used to extend privacy in SMC operations. [8] Frameworks can be used to solve general privacy-preserving problems.

4.1. Towards SMC collaborated with cloud

Though SMC is best suited for many applications like secret e-voting, privacy preserved healthcare data mining, financial solutions, The communication delay and the computations cost makes it not very much practical approach. Many of the SMC algorithms are good in theory and practically impossible as the scalability of the applications. Since the evolution of the cloud the scenario changed. SMC has now a better place to host the computations where the network and communication related issues will be maintained by Cloud Service Provider (CSP). Several researchers [14] [26] have proposed the outsourcing SMC to the cloud.

The efficiency of SMC protocols will be improved and expenditure will be reduced. This gives the great interest to the researchers to opt for cloud based architecture for SMC computations. However migrating computation into cloud yields to unreliable third party situation we’ve discussed earlier. Fully Homomorphic Encryption [14] enables users to share encrypted data rather than plain text. The output function will be computer over cipher text. Re Encryption [11], secure sum protocol [5] techniques are proposed to ensure the privacy in sharing the user sensitive data into the cloud environment. [12] Detailed the model with FHE applied with cloud computing to enhance privacy.

Table 1 details about comparison of various SMC models considering important parameters like computational cost, centralized supervision and transparency details and SMC development approach.

Table 1: A Comparative Analysis of Various SMC Approaches

Mechanism	Number of players	Circuit Approach	Encryption approach	Computation overhead	Trusted Third Party Required	Re Encryption	Transparency	Privacy
Yao’s Two Party computation[1]	2	√	X	low	√	×	×	L
Goldreich GMW Circuits[2]	N	√	X	Low	√	×	×	L
Re encryption Technique[11]	n	×	√	Very High	√	√	×	√
Homomorphic Encryption[14]	n	×	√	High	√	x	×	√
Fully Homomorphic Encryption[14]	n	×	√	Very High	√(Semi honest)	×	×	√
SMC with Cloud architecture [14] [26]	n	×	√	Outsourced	Unreliable	x	x	√
Block Chain technology	-	×	x	Medium	x	×	√	x

Notations: n- Multi party, L – Limited.

5. Conclusions

In this paper we discussed the overview of secure multi-party computation and its evolution till recent advancements. We also highlighted that SMC in collaboration is very handy in solving complex computations and keeping private user data safe. This is vital in current mobile world where user data is being share by several applications to unknown sources. We also presented comparative analysis of various SMC protocols on various factors which highlights the research gap in untrustworthy TTP situations. Audit trail and verifiability are various other factors researchers can focus on.

Acknowledgement

We thank KLEF for providing excellent research environments and the department of CSE for extending hand in continuing our research work.

References

[1] Yao, Andrew C. "Protocols for secure computations." Foundations of Computer Science, 1982. SFCS'08. 23rd An-nual Symposium on. IEEE, 1982.

[2] Goldreich, Oded. "Secure multi-party computation." Manuscript. Preliminary version (1998): 86-97.

[3] Marwan, Mbarek, Ali Kartit, and Hassan Ouahmane. "Applying secure multi-party computation to improve collab-oration in healthcare cloud." Systems of Collaboration (Sys-Co), International Conference on. IEEE, 2016.

[4] Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." (2011).

[5] I. Jahan, N. N. Sharmy, S. Jahan, F. A. Ebha and N. J. Lisa, "Design of a secure sum protocol using trusted third party system for Secure Multi-Party Computations," 2015 6th International Conference on Information and Communication Systems (ICICS), Amman, 2015, pp. 136-141.

[6] Lapets, Andrei, et al. Secure multi-party computation for analytics deployed as a lightweight web application. Comput-er Science Department, Boston University, 2016.

[7] Maurer, Ueli. "Secure multi-party computation made simple." Discrete Applied Mathematics 154.2 (2006): 370-381.

[8] Y. Lindell and B. Pinkas, "Secure Multiparty Computation for Privacy- Preserving Data Mining," The Journal of Privacy and Confidentiality, vol. 1, no. 1, pp. 59-98, 2009.

[9] Gordon, S. Dov, Feng-Hao Liu, and Elaine Shi. "Con-stant-round MPC with fairness and guarantee of output deliv-ery." Annual Cryptology Conference. Springer, Berlin, Hei-delberg, 2015.

[10] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In CRYPTO ’88: Proceedings on Advances in cryptology, pages 27–35, New York, NY, USA, 1990. Springer-Verlag New York, Inc

[11] Tysowski, Piotr K., and M. Anwarul Hasan. "Re-Encryption-Based Key Management towards Secure and Scalable Mobile Applications in Clouds." IACR Cryptology EPrint Archive 2011 (2011): 668.

[12] Tebaa, Maha, and Said El Hajji. "Secure cloud compu-ting through homomorphic encryption." arXiv preprint arXiv: 1409. 0829 (2014).

[13] Yao, Yuangang, et al. "Efficiently secure multiparty computation based on homomorphic encryption." Cloud Computing and Intelligence Systems (CCIS), 2016 4th Inter-national Conference on. IEEE,2016

[14] López-Alt, Adriana, Eran Tromer, and Vinod Vaikun-tanathan. "On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption." Proceedings of the forty-fourth annual ACM symposium on Theory of com-puting. ACM, 2012.

[15] Kamara, Seny, and Mariana Raykova. "Secure out-sourced computation in a multi-tenant cloud." IBM Work-shop on Cryptography and Security in Clouds. 2011.

[16] Kosba, Ahmed, et al. "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts." Secu-rity and Privacy (SP), 2016 IEEE Symposium on. IEEE, 2016.

[17] Hamlen, Kevin, et al. "Security issues for cloud compu-ting." Optimizing information security and advancing privacy assurance: new technologies: new technologies 150 (2012).

[18] Ben-David, Assaf, Noam Nisan, and Benny Pinkas. "FairplayMP: a system for secure multi-party computation." Proceedings of the 15th ACM conference on Computer and communications security. ACM, 2008.

[19] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In CRYPTO ’88: Proceedings on Advances in cryptology, pages 27–35, New York, NY, USA, 1990. Springer-Verlag New York, Inc.

[20] Rabin, Michael O. "How to Exchange Secrets with Oblivious Transfer." IACR Cryptology ePrint Archive 2005 (2005): 187. .

[21] O. Goldreich, the Foundations of Cryptography - Vol-ume 2, Basic Applications. Cambridge University Press, 2004.

[22] Cramer, Ronald, Ivan Damgård, and Yuval Ishai. "Share conversion, pseudorandom secret-sharing and applications to secure computation." Theory of Cryptography Conference. Springer, Berlin, Heidelberg, 2005.

[23] Hazay, Carmit, and Yehuda Lindell. "Semi-honest Ad-versaries." Efficient Secure Two-Party Protocols. Springer, Berlin, Heidelberg, 2010. 53-80.

[24] Subashini, and Veeraruna Kavitha. "A survey on securi-ty issues in service delivery models of cloud computing." Journal of network and computer applications 34.1 (2011): 1-11.

[25] https://www.rightscale.com/lp/2017-state-of-the-cloud-report

[26] Kamara, Seny, Payman Mohassel, and Mariana Rayko-va. "Outsourcing Multi-Party Computation." IACR Cryptolo-gy ePrint Archive 2011 (2011): 272.