A Secure Multiparty Computation scheme using Homomorphic Elliptic Curve Cryptography

[1]Anupam kumari
Department of Computer science &Engineering,.
Vadodara ,india
Kumarianupam000@gmail.com

[2]Ankit Chouhan
Dept. of Computer Science & Engineering
Vadodara,india
ankit.chouhan@paruluniversity.ac.in

[3]Makhduma saiyad
Dept.of computer science &amp;engineering
Vadodara ,india
Makhduma.saiyad2810@paruluniversity.ac.in

1,2,3 Parul institute of engineering and technology (PIET)VADODARA

Abstract - In this system, we attention on Elliptic Curve Cryptography based method for Secure Multiparty Computation (SMC) problem. Extensive creation of data and the growth of communication tools have enabled collaborative additions among gatherings in distributed scenario. Preservative isolation of data retained by gatherings is critical in such situations. Classical approach to SMC is to perform addition using Trusted Third Party (TTP). However, in functional situation, TTPs are hard to achieve and it is imperious to remove TTP in SMC. In addition, existing solutions proposed for SMC use classical homomorphism encryption systems such as RSA and Paillier. Due to the advanced cost experienced by such cryptosystems, the resultant SMC procedures are not scalable. We propose Elliptic Curve Cryptography (ECC) based approach for SMC that is scalable in terms of computational and statement cost and avoids TTP. In literature, there do exist various ECC based homomorphic schemes and it is imperious to consider and evaluate these systems in order to select the suitable for a given application.

I. INTRODUCTION

Our handhelds have become smaller; computers faster; disks larger; networks more effective and we enjoy bandwidths like never before; everything grew exponentially. All this calculations up to a very promising situation for data collection, transmission and storage. In order to fully consume this data, there is a need to achieve cooperative calculation on data. However, the data composed mostly comprise info related to persons, their economic status, lifestyle and social behavior in general. Joint calculation on data may attitude threat to confidentiality of person's data. Hence, there is a need to protocol a method that does joint calculation on private data without revealing data to other parties.

In order to make available a well-organized allocation protocol in the elliptic-curve setting we have reentered the literature on elliptic-curve point additions. Usually these algorithms try to reduce the number of field operations done, whereas in our setting we want to have the lowest possible multiplicative depth. We show that a recent algorithm, gives an algorithm that fits perfectly the homomorphism encryption setting with only two levels of multiplications.

II. LITERATURE SURVEY

Sr. No.	Paper Name	Author Name	Published Year	Description
1.	Secure and Practical Outsourcing of Linear Programming in Cloud Computing: A Survey	V. Sudarsan Rao, N. Satyanarayana, PhD	2017	In this paper, the essential terms involved in the cloud security has been presented. Whereas, the privacy cheating discouragement ”Seccloud”, is used for achieving the greater aspects of security. Although the cloud computing is being used to outsource large-scale computations to the cloud, data privacy has become a major issue.
2.	Computation on Encrypted Data using Data Flow Authentication	Andreas Fischer, Benny Fuhry	2017	Encrypting data before sending it to the cloud protects it against hackers and malicious insiders, but requires the cloud to compute on encrypted data.
3.	Private Intersection-Sum Protocol with Applications to Attributing Aggregate Ad Conversions	Mihaela Ion, Ben Kreuter, Erhan Nergiz	2017	In this work, we consider the Intersection-Sum problem: two parties hold datasets containing user identifiers, and the second party additionally has an integer value associated with each user identifier.
4.	A Practical Client Application Based On Attribute-Based Access Control For Untrusted Cloud Storage	Julian Jang-Jaccard	2016	One of widely used cryptographic primitives for the cloud application is Attribute Based Encryption (ABE) where users can have their own attributes and a ciphertext encrypted by an access policy.

III. EXISTING SYSTEM

We attention on Elliptic Curve Cryptography based method for Secure Multiparty Computation (SMC) . Prevalent propagation of data and the growth of communication skills have enabled cooperative additions among gatherings in dispersed condition. Preserving privacy of data possessed by parties is critical in such scenarios. Traditional approach to SMC is to perform addition using Trusted Third Party.

IV. PROPOSED SYSTE

We propose Elliptic Curve Cryptography (ECC) based method for SMC that is accessible in positions of computational and message cost and evades TTP.In our proposed method we focus on enhance the security label over an insecure channels.

V. CONCLUSION

In this system, we propose method to securing multiparty computation using elliptic curve cryptography. We empirically evaluated various encryption schemes for our proposed protocol. We found that ECC based algorithm achieves better among these algorithms. We decorated various applications such as privacy preserving data mining as the candidate applications for our proposed approaches.

REFERENCES

[1] O. Goldreich, "The Foundations of Cryptography," Vol. 2. Cambridge Univ. Press, Cambridge, 2004.

[2] Y. Lindell and B. Pinkas, "Secure Multiparty Computation for Privacy-Preserving Data Mining," Journal of Privacy and Confidentiality, Vol. 1, No. 1, 2009, pp. 59-98.

[3] M. Rabin, "How to Exchange Secrets by Oblivious Transfer," Technical Report Tech. Memo TR-81, Aiken Computation Laboratory, 1981.

[4] D. Josep Ferrer, "A new privacy homomorphism and applications," Information Processing Letters, Vol. 60, No. 5, 1996, pp. 277-282. http://dx.doi.org/10.1016/S0020-0190(96)00170-6

[5] A. Shamir, "How to Share a Secret," Communication of the ACM, Vol. 22, No. 11, 1979, pp. 612-613. http://dx.doi.org/10.1145/359168.359176

[6] T. B. Pedersen, Y. Saygin and E. Savas, "Secret Sharing vs. Encryption-Based Techniques for Privacy Preserving Data Mining," UNECE/Eurostat Work Session on SDC, 2007.

[7] S. Patel, S. Garasia and D. Jinwala, "An Efficient Approach for Privacy Preserving Distributed K-Means Clustering using Shamir's Secret Sharing Scheme," In: T. Dimitrakos, R. Moona and D. Patel, Eds., Trust Management VI, IFIP Advances in Information and Communication Technology, Vol. 347, Springer, Boston, 2012, pp. 129-144.

[8] G. Jagannathan and R. N. Wright, "Privacy-Preserving Distributed k-Means Clustering over Arbitrarily Partitioned Data," KDD, ACM Press, 2005, pp. 593-599.

[9] S. Jha, L. Kruger and P. McDaniel, "Privacy Preserving Clustering," 10th European Symposium on Research in Computer Security, 2005, pp. 397-417.

[10] N. Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation, Vol. 48, 1987, pp. 203-209

[11].Dindayal mahto,Danish Ali khan "Security analysis of elliptic curve cryptography and RSA",vol-1,WCE 2016