

# SMC Protocol for Privacy Preserving in Banking Computations Along with Security Analysis

Rohit Pathak<sup>‡</sup>, Satyadhar Joshi<sup>†</sup>

<sup>‡</sup> Acropolis Institute of Technology & Research, Indore, M.P., India  
<sup>†</sup> Shri Vaishnav Institute of Technology & Science, Indore, M.P., India  
rohitpathak@ieee.org, satyadhar\_joshi@ieee.org

**Abstract-** The expansion of internet escalated banking to a new level and has raised tremendous opportunities of joint transactions in which multiple banks cooperatively conduct some computation. Such computations use confidential data of the involved banks to compute the result. As the concerned data is private for the owning organization, its security is prime concern. Privacy preservation concern rises as no party can be trusted enough to know all the inputs of computation. In this paper we have proposed a scalable and efficient protocol to perform secure multi-party computations on encrypted data. The process involves encrypting data in a manner that it does not affect the result of the computation. Virtual parties are created by all organizations and encrypted data is distributed among them. Modifier tokens are generated along encryption which are assigned to virtual parties, and finally used in the computation. The computation function uses the acquired data and modifier tokens to compute result. As the data involved in computation was encrypted, without revealing the data right result can be computed and privacy of the parties is maintained. The protocol is highly efficient in conducting banking computations. We have analyzed the security and complexity of protocol and shown how zero hacking security can be achieved. Also we have analyzed the performance through various tests.

**Keywords-** Secure Multi-Party computation, Communication and Information Security

## I. INTRODUCTION

With the advent into the 20th century the expansion of internet has escalated banking to a new level. The World Wide Web is becoming more reliable each passing day. A large ratio of population is relying on it for their daily work. Internet has penetrated into the banking industry deeply and nearly every desired transaction can be performed online. Fund transfer, payments, shopping and many other types of transaction are possible just with a few clicks. Internet and communication between different banks has given rise to a new banking structure. In this new banking era there are numerous opportunities when there is a need to perform a joint transaction between two or more parties or banks. There may be a need to perform survey's involving confidential data from different banks and other organizations. Banks may be outsourcing their work to BPO organizations.

Security and privacy are the two major issues needed to be addressed by the banking industry to have an increased rate of customers banking online. Another important issue is about sharing information with other banks and organizations to

ensure that data and vital information of the concerned customer or the bank is secured and protected. What does security actually mean, in the context of banking, and how is it different from privacy? Is it even different? Are security concerns any different for a multinational bank or national bank, and is the customer or the online service provider ultimately held responsible in the event of failure? One thing's for sure – as organizations and common people continue to broadly adopt online banking as a strategy to perform their transactions and other processes, concerns around security take on an entirely different dimension.

Today's online banking systems have amplified and broadened security needs to the extent that security concerns now overarch all other IT-enabled sectors. Security has been a banking concern since long before online banking started and enabled customers of the processes and capabilities online. Security is not just a consequential incident that results from proliferation of information technology. Prior to IT-enabled banking, the definition of security was more passive – the state of being safe or secure. Usually the types of security topics & questions discussed in the context of banking are that who physically altered what accounts, where the accounts or money was stored and how they were transported there were usually.

There is an absence of proper data security and cyber laws which is encumbering banking and its business prospects. There is also tremendous hype and a lack of understanding of the issues surrounding security. The most significant security issues revolve around the protection of data in one manner or another. Some of the information security and data privacy challenges that banks face include lack of stringent data protection laws, use of portable devices such as laptops by employees to store confidential information, rising data security costs due to increased employee background checks, training employees in maintaining data security, ensuring compliance with security policies implemented in the company, and systemic plugging of any loopholes through employee activity monitoring procedures. To ensure that the confidentiality of a customer or bank's information is maintained, there is need to implement data security measures, which can be classified into measures taken at the recruitment level and measures taken at the operational level.

## II. RECENT WORKS

not breach the security. The data is encrypted and can only be used for computation and exact values can never be obtained from it.

#### CONCLUSION

Thus we have shown another application of the powerful VPP protocol in banking applications. We know that with the advent into the 20th century, the expansion of the World Wide Web has escalated banking to a new level. Tremendous opportunities for joint transactions have arisen in which multiple banks cooperatively conduct some computation. Security and privacy preserving measures are major issues regarding such cases as confidential data is concerned. We proposed a secure protocol for multi-party computations in which privacy of individual is preserved. We have corroborated that by creating fake data and distributing it among the generated virtual parties then sending this data along with modifier tokens to carry out computations on encrypted data using an improvised computation method, we can achieve zero hacking security. Hiding the identity of parties using anonymizer and reaching zero hacking security has been substantiated. The protocol and algorithm are highly scalable and optimized for computations of surveys, banking, business etc. Encryption methods have been built for certain common functions and the process of generating modifier tokens for a collective method has been shown. SMC's are used for many big surveys and large scale statistical calculations. With the use of VPP most of the statistical calculations and other computations can be performed without revealing the data to other parties and even to the third party. It can allow us to reach zero hacking security for a wide variety of applications. Using this protocol and algorithm a wide variety of computations can be optimally performed with enhanced security and privacy.

#### REFERENCES

- [1] Yao Andrew C., "Protocols for secure computations," *Proc. of 23rd Annual Symposium Foundations of Computer Science*, pp. 160-164.
- [2] Mikhail A., Marina B., Jiangtao L., Keith F., Mercan T., "Private collaborative forecasting and benchmarking," *Proc. of the 2004 ACM workshop on Privacy in the Electronic Society*, 2004.
- [3] Mikhail A., Marina B., Jiangtao L., Keith F., Mercan T., "Private collaborative forecasting and benchmarking," *Proc. 2004 ACM workshop on Privacy in the electronic society*, pp. 103-114, 2004.
- [4] Wenliang Du, Zhijun Zhan, "A practical approach to solve secure multi-party computation problems," *Proc. of the New Security Paradigms Workshop*, 2002.
- [5] Linda M.N., Johnny W., "A unified approach for multilevel database security based on inference engines," *Transaction of ACM New York*, Vol. 21, Issue 1, Feb 1989.
- [6] Wenliang D., Atallah M.J., "Privacy-preserving cooperative scientific computations," *Proc. 14th IEEE Computer Security Foundations Workshop*, Jun 11-13 2001, pp. 273 - 282.
- [7] Ran C., Uri F., Oded G., Moni N., "Adaptively secure multi-party computation," *Proc. The 28th annual ACM symposium on Theory of computing*.
- [8] Mikhail J.A., "Secure and Private Sequence Comparisons," *Proc. The 2003 ACM workshop on Privacy in the electronic society*, 2003.
- [9] Atallah, M.J., Elmongui H.G., Deshpande V., Schwarz L.B., "Secure supply-chain protocols," *Proc. IEEE International Conference, E-Commerce*, 2003.

- [10] Ueli M., "The role of cryptography in database security," *Proc. The 2004 ACM SIGMOD international conference on Management of data*, 2004.
- [11] Rakesh A., Ramakrishnan S., "Privacy-Preserving Data Mining," *Proc. The ACM SIGMOD Conference on Management of Data*, 2000.
- [12] Mishra D.K., Chandwani M., "Extended protocol for secure multi-party computation using ambiguous identity," *WSEAS Transactions on Computer Research, Greece*, Vol. 2, No. 2, pp. 227-233, Feb. 2007.
- [13] Mishra D.K., Chandwani M., "Arithmetic cryptography protocol for secure multi-party computation," *Proc. Of IEEE SoutheastCon 2007: The International Conference on Engineering - Linking future with past, Richmond, Virginia, USA*, pp. 22-24, 22-25 Mar. 2007.
- [14] Mishra D.K., Chandwani M., "Anonymity enabled secure multi-party computation for Indian BPO," *Proc. of the IEEE Tenccon 2007: International conference on Intelligent Information Communication Technologies for Better Human Life, Taipei, Taiwan*, pp. 52-56, 29 Oct. - 02 Nov. 2007.
- [15] Rohit P., Satyadhar J., "Secure Multi-party Computation Using Virtual Parties for Computation on Encrypted Data," *Advances in Information Security and Assurance, Springer Lecture Notes on Computer Science, Springer Berlin / Heidelberg*, Vol. 5576/2009, Jun. 2009, DOI=10.1007/978-3-642-02617-1\_42.
- [16] Rohit P., Satyadhar J., "Secure Multi-party Computation Protocol for Defense Applications in Military Operations using Virtual Cryptography," *Contemporary Computing, Communications in Computer and Information Science, Springer Berlin Heidelberg*, Vol. 40, 17-19 Aug. 2009, DOI=10.1007/978-3-642-03547-0\_37.
- [17] Rohit P., Satyadhar J., "Secured Communication for Business Process Outsourcing using Optimized Arithmetic Cryptography Protocol based on Virtual Parties," *Contemporary Computing, Communications in Computer and Information Science, Springer Berlin Heidelberg*, Vol. 40, 17-19 Aug. 2009, DOI=10.1007/978-3-642-03547-0\_20.
- [18] Rohit P., Satyadhar J., "Secure Multi-Party Computation Protocol for Statistical Computation on Encrypted," *Proc. of 2009 International Conference on Software Technology and Engineering (ICSTE 2009)*, 24-26 Jul. 2009.