www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issues 6 June 2016, Page No. 16778-16781

Preserving Data Privacy without Secure Channel

Nitha Sagar J[1], Spandana G M[2],

[1]Department Of Information Science and Engineering,
The National Institute of Engineering, Mysuru, India.
nithasagar16@gmail.com

[2]Deparment of Information Science and Engineering,
The National Istitute of Engineering, Mysuru, India.
Spandy2694@gmail.com

Abstract: ***The main objective is to preserve data privacy during communication. In this paper, we show how external aggregators or multiple parties use algebraic statistics over their private data without exploiting data privacy assuming all channels and communications are open to eavesdropping attacks. Firstly, we propose many protocols that guarantee data privacy. Later we propose advanced protocols that tolerate maximum of k passive adversaries who do not try to modify the computation.***

Keywords: data privacy, external aggregators, secure channel, SMC.

1. INTRODUCTION

The problem of Privacy-preserving data aggregation has been a hot research issue in the field of cryptography from a very long time. In several real life applications such as crowd sourcing or mobile cloud computing, individuals have to provide their sensitive data (location-related or personal-information-related) to receive specific services from the entire system. In the existing system, there is chance of original data being hacked since communication is between two users only (i.e, between the sender and the receiver). At present, SMC is being used to keep the individual's data secret. Secure Multi-party Computation (SMC) was first introduced by Yao in 1982 as Secure Two-Party Computation. Only one uniform result could be given as output by the SMC function to all or parts of participants, which is the algebraic aggregation of their input data. Even though it appears like the privacy-preserving data aggregation problem gets solved by this approach, this actually does not completely solve our problem. Some of the disadvantages of the existing system are: 1) Interactive invocation is required for participants in synchronous SMC which leads to high communication and computation complexity. Even in the asynchronous SMC, the computation complexity is still too high for practical applications. 2) Homomorphic Encryption (HE) allows direct addition and multiplication of cipher texts while preserving decryptability. One could also try to solve our problem using this technique, but HE uses the same decryption key for original data and the aggregated data That is, the operator who executes homomorphic operations upon the cipher texts are not authorized to achieve the final result. This forbids aggregator from decrypting the aggregated result, because if the aggregator is allowed to decrypt the final result, he can also decrypt the individual cipher text received, which contradicts our motivation. Also, because the size of the plaintext space is limited, the number of addition and multiplication operations executed upon cipher texts was limited. 3) The complexity of general HE is too high to use in real application. Naehrig et al. also proposed a HE scheme which sacrificed possible number of multiplications for speed, but it still needs too much time to execute homomorphic operations on cipher texts. Besides the aforementioned drawbacks, both SMC and HE require an initialization phase during which participants request keys from key issuers via secure channel. This could be a security hole since the security of those schemes relies on the assumption that keys are disclosed to authorised participants only. The goal is to design efficient protocols without relying on a trusted authority and secure pair wise communication channels. The main contributions of this paper are:

1) Formulation of a model without secure channel or trusted center: Different from many other models in privacy preserving data aggregation problem, our model does not require a secure communication channel nor a trusted central key issuer.

2) Efficient protocol in linear time: The total communication and computation complexity of our work is proportional to the number of participants' n, while the complexities of many similar works are proportional to n^2. We do not use complicated encryption protocols, which makes our system much faster than other proposed systems.

3) Secure sum and product calculation: We generalize the privacy-preserving data aggregation to multivariate sum and product calculation whose inputs are jointly provided by multiple parties. That is, our scheme enables multiple parties to securely compute.

4) Tolerate up to k collusive adversaries: Our protocol is robust against up to k colluding passive adversaries who do not try to tamper the computation.

2. RELATED WORK

There has been a considerable amount of work on how to preserve data privacy. Some of the related work in this field include:

1) Achieving differential privacy of data disclosure in the smart grid

The smart grid poses new privacy issues to individuals because of the fine-grained usage data collection. For instance, smart

metering data might present super accurate real-time home appliance energy load using which, human activities inside the houses can be monitored. Battery-based Load Hiding (BLH) is one of the ways to effectively hide battery loads from outsiders. In BLH, a battery that is installed for each household is smartly controlled to store and supply power to the appliances. Inspite of such technique being proved useful in preventing certain types of attacks, none of existing BLH works give mechanisms to preserve privacy. In this work, the privacy of smart meters is investigated using differential privacy. First, an analysis of the current existing BLH methods is carried out to show that they fail to guarantee differential privacy in the BLH problem. Finally, BLH algorithm is proposed that successfully assures differential privacy, and further propose the Multitasking-BLH-Exp3 algorithm which updates the BLH algorithm based on the context and the constraints. Results obtained after extensive simulations show that the proposed method is effective and efficient when compared to the current BLH methods..

2) *Verifiable private multiparty computation: ranging and ranking*

Work such as set operations, ranking etc that are currently existing in the field of distributed SMC mainly give importance to privacy issues and ignore other aspects such as inputs and outcomes. Existing work wrongly assumes that the parties involded in computation follow the protocol honestly but in practice, there are malicious attacks that take place to forge input or even lie about the result and so on. This work however focuses on the verification of such computation. A thorough analysis of attacks on privacy preserving SMC approaches are carried out and on that basis, protocols that are proved to be both verifiable as well as privacy preserving are designed for existing works. These protocols are then implemented on laptops and mobile phones. The results show the efficiency of these protocols.

3) *Privacy preserving aggregation of time-series data*

Keeping in mind how an untrusted data aggregator can use methods over various participants' data, without compromising each individual's privacy. A method is proposed that enables group of participants to upload their part of encryption to a data aggregator, that allows the aggregator to compute the values of all participants' data, but at the same time, makes sure the aggregator does not learn about anything else. Desirable privacy properties are obtained using two techniques. First, the aggregator makes use of cryptographic techniques to decrypt the sum from various cipher texts using different user keys. Second, some procedures are introduced to ensure the outcome statistic is kept private despite of compromising few participants.

4) *Search me if you can: privacy-preserving location query service*

With growth and improvement in technologies such as smart phone technology, location based service is gaining popularity equally rapidly. Its Useful functionalities have been successful in attracting users. The location information of users are considered by the LSB providers to offer appropriate functions to those users. However, LBS could lead to privacy issues since location information alone contains plethora of information regarding the user. Therefore, exploiting the usefulness of LBS while preserving privacy is quite challenging. This work introduces protocols that help overcome the above challenges.

3. PROPOSED MODEL

We reconsider the privacy preserving data aggregation problem. The goal is to design protocols that work efficiently without depending on a trusted authority and secure communication channels. The main contributions are: Formulation of a model without secure channel or trusted center: Different from many other models in privacy preserving data aggregation problem, our model does not require a secure communication channel nor a trusted central key issuer.

1) Efficient protocol in linear time: The total communication and computation complexity of our work is proportional to the number of participants n, while the complexities of many similar works are proportional to n2. We do not use complicated encryption protocols, which makes our system much faster than other proposed systems.

2) Secure sum and product calculation: We generalize the privacy-preserving data aggregation to multivariate sum and product calculation whose inputs are jointly provided by multiple parties.

3) Tolerate up to k collusive adversaries: Our protocol is robust against up to k colluding passive adversaries who do not try to tamper the computation. The rest of the paper is organized as follows. We present the system model and necessary background. We analyze the needed number of communications with secure communication channels when users communicate randomly. We address the privacy preserving sum and product calculation by presenting two efficient protocols. Then, we present detailed security analysis of our protocols and the performance evaluation is reported.

4) Finally, solutions to various problems based on our protocols are presented.

3.1 Flow charts

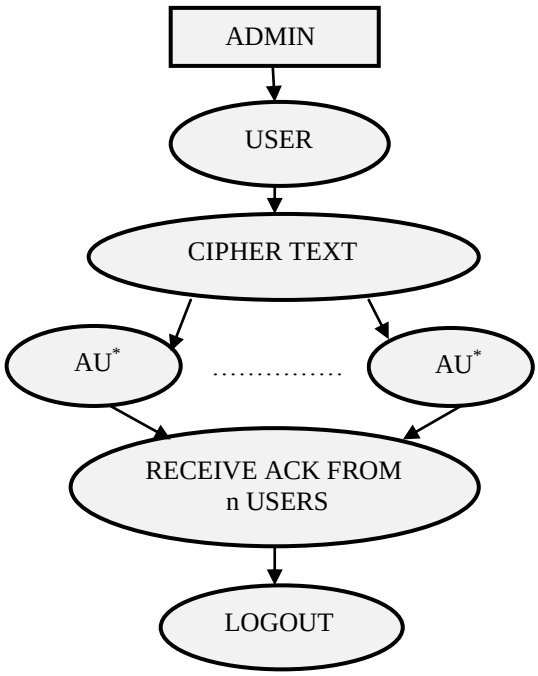

Figure 1: Data Flow diagram for Admin.

*Authenticated User

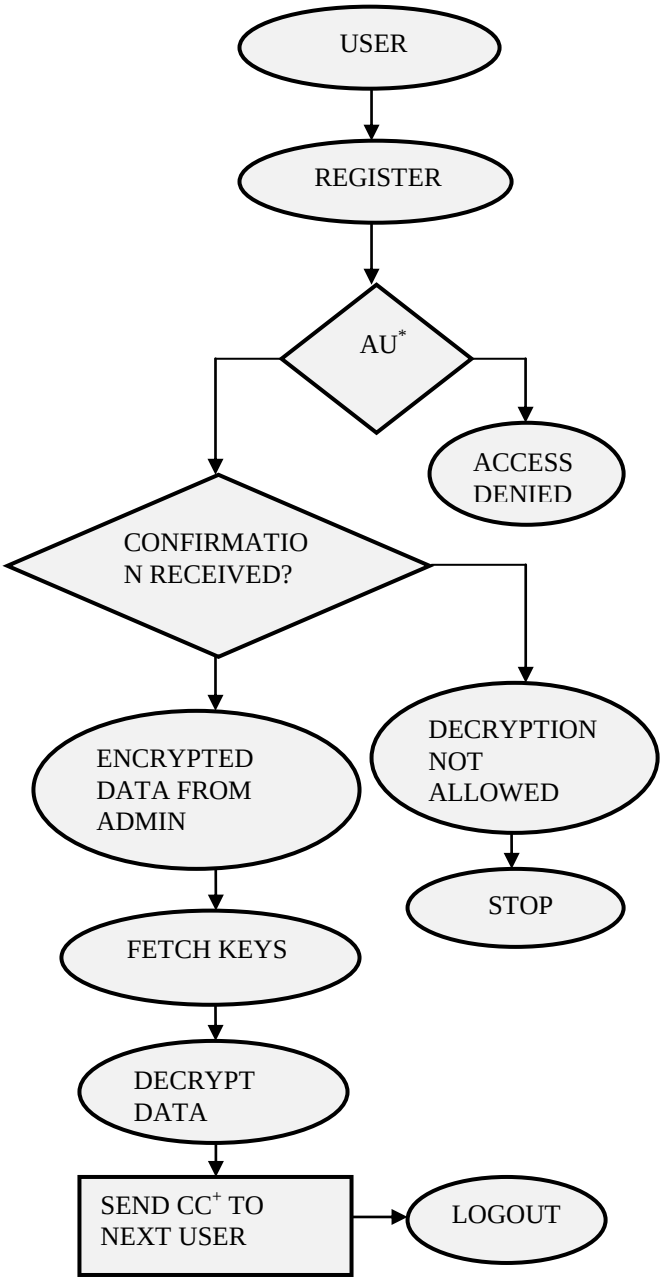

Figure 2: Data Flow diagram for User

The advantages of this system are:

1) 1) Protection is provided against the attackers since the key is not passed through the confidential channels and the key is known only to the admin and the users who are participating in it.
2) 2) If the confirmation code is not received by the current user from the previous user, then we can predict that something has gone wrong and take corrective actions

+Confirmation Code

4. CONCLUSION

In this paper, we successfully achieve privacy-preserving sum and product calculation protocols without secure communication channels or trusted key issuers. We allow up to k (adjustable parameter) collusive participants who will not tamper the computation but try to manipulate their parameters to infer others' private values. We formally analyzed the security of our protocols and showed that the protocols are secure if the CDH problem is assumed to be intractable, and we also showed with implementation that the protocols are efficient to be applicable in real life. At the end, we propose numerous applications that are achieved from our protocols. One of our future works is to design privacy preserving data releasing protocols such that general function of data can be evaluated correctly while preserving individuals' data privacy

References

[1] C. C. Aggarwal and S. Y. Philip, A general survey of privacypreserving
data mining models and algorithms. Springer, 2008.
[2] D. Beaver, S. Micali, and P. Rogaway, "The round complexity of
secure protocols," in STOC. ACM, 1990.
[3] A. Ben-David, N. Nisan, and B. Pinkas, "Fairplaymp: a system
for secure multi-party computation," in CCS. ACM, 2008.
[4] D. Boneh, "The decision diffie-hellman problem," Algorithmic
Number Theory, 1998.
[5] C. Castelluccia, A. Chan, E. Mykletun, and G. Tsudik, "Efficient
and provably secure aggregation of encrypted data in wireless
sensor networks," Transactions on Sensor Networks (TOSN), 2009.
[6] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation
of encrypted data in wireless sensor networks," in MobiQuitous.
IEEE, 2005.
[7] T.-H. H. Chan, E. Shi, and D. Song, "Privacy-preserving stream
aggregation with fault tolerance," in Financial Cryptography and
Data Security (FC). Springer, 2012.
[8] X. Chen, X. Wu, X.-Y. Li, Y. He, and Y. Liu, "Privacy-preserving
high-quality map generation with participatory sensing," in INFOCOM.
IEEE, 2014.
[9] C. Clifton, M. Kantarcioglu, J. Vaidya, X. Lin, and M. Zhu,
"Tools for privacy preserving distributed data mining," SIGKDD
Explorations Newsletter, 2002.
[10] C. Dwork, "Differential privacy," in Automata, languages and
programming. Springer, 2006.
[11] C. Dwork and J. Lei, "Differential privacy and robust statistics,"
in STOC. ACM, 2009.
[12] B. Edelman, M. Ostrovsky, and M. Schwarz, "Internet advertising
and the generalized second price auction: Selling billions of dollars

worth of keywords," National Bureau of Economic Research, Tech. Rep., 2005.
[13] B. J. Falkowski, "A note on the polynomial form of boolean
functions and related topics," Transactions on Computers, 1999.
[14] N. Fazio, R. Gennaro, I. M. Perera, andW. E. Skeith III, "Hardcore
predicates for a diffie-hellman problem over finite fields." 2013.
[15] J. Feigenbaum and M. Merritt, Distributed Computing and Cryptography:
Proceedings of a Dimacs Workshop October 4-6, 1989. AMS Bookstore, 1991.
[16] M. Fischlin, "A cost-effective pay-per-multiplication comparison
method for millionaires," in Topics in CryptologyCT-RSA 2001.
Springer, 2001.
[17] A. Friedman and A. Schuster, "Data mining with differential
privacy," in SIGKDD. ACM, 2010.
[18] B. Fung, K. Wang, R. Chen, and P. S. Yu, "Privacy-preserving
data publishing: A survey of recent developments," Computing Surveys (CSUR), 2010.
[19] C. Gentry, "Fully homomorphic encryption using ideal lattices,"
in STOC. ACM, 2009.
[20] C. Gentry and S. Halevi, "Implementing gentrys fullyhomomorphic
encryption scheme," Advances in Cryptology–EUROCRYPT, 2011.
[21] O. Goldreich, "Secure multi-party computation," Manuscript. Preliminary
version, 1998.
[22] S. Goryczka, L. Xiong, and V. Sunderam, "Secure multiparty
aggregation with differential privacy: a comparative study," in Proceedings of the Joint EDBT/ICDT 2013 Workshops. ACM, 2013.
[23] W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher,
"Pda: Privacy-preserving data aggregation in wireless sensor networks," in INFOCOM. IEEE, 2007.
[24] M. Jawurek and F. Kerschbaum, "Fault-tolerant privacy preserving statistics," in PETS. Springer, 2012

.Author Profile

<Author Photo>

Taro Denshi received the B.S. and M.S. degrees in Electrical Engineering from Shibaura Institute of Technology in 1997 and 1999, respectively. During 1997-1999, he stayed in Communications Research Laboratory (CRL), Ministry of Posts and Telecommunications of Japan to study digital beam forming antennas, mobile satellite communication systems, and wireless access network using stratospheric platforms. He now with DDI Tokyo Pocket Telephone, Inc.