Eurasian Journal of Analytical Chemistry
ISSN: 1306-3057 OPEN ACCESS 2017 12 (4): 259-264

Secure Multiparty Protocols

K. Anita Davamani, S. Amudha

Received: 12 December 2016 ▪ Revised: 15 January 2017 ▪ Accepted: 14 February 2017

Abstract: Secure Multiparty Computation (SMC) protocols are one of the first techniques used in privacy preserving data mining in distributed environments. The protocol does not reveal anything other than the output of the function or anything that can be computed from it in polynomial time. Moreover, the protocol does not require a trusted third party. The main focus of this paper is to design the look ahead approach for SMC protocol with the help of distributed k-anonymity technique. These protocols prevent information disclosure other than the objective function. People are jointly conducting computation tasks based on the private inputs they each supplies. These computations could occur between mutually un-trusted parties, or even between Secure Multiparty Computations (SMC). The look-ahead operation is highly localized and its accuracy depends on the amount of information the parties are willing to share.

Keywords: Privacy, Secure Multiparty Computation, Anonymity Technique.

INTRODUCTION

Secure multiparty computation (SMC) protocols are one of the first techniques used in privacy preserving data mining in distributed environments. The idea behind these protocols is based on theoretical proof that two or more parties, both having their own private data, can collaborate to calculate any function on the union of their data [8]. While doing so, the protocol does not reveal anything other than the output of the function or anything that can be computed from it in polynomial time. More-over, the protocol does not require a trusted third party. While these properties are Promising for privacy preserving applications, SMC may be prohibitively expensive. In fact, many SMC protocols for privacy preserving data mining suffer from high computation and communication costs. Furthermore, those that are closest to be practical are designed for the semi honest model, which assumes that parties will not deviate from the protocol. Theoretically, it is possible to convert protocols in the semi honest model into protocols in the malicious model. However, the resulting protocols are even more costly. To the best of our knowledge, this is the first work that looks ahead of an SMC protocol and gives an estimate for We state that an ideal look ahead satisfies the following:

1. The methodology is highly localized in computation, it is fast and requires little communication cost (at least asymptotically better than the SMC protocol).
2. The methodology relies on non sensitive data, or better, data that would be implied from the output of the objective function.

RELATED WORKS

In this section, we outline a number of characteristics we consider crucial to the design of a practical privacy criterion. At the same time, we review the literature, indicating how previous work does not match our desired characteristics. From our perspective, a practical privacy criterion should display the following.

Characteristics

1. Intuitive: The data owner (usually not a computer scientist) should be able to understand the privacy criterion in order to set the appropriate parameters.
2. Efficiently checkable: Whether a release candidate satisfies the privacy criterion should be efficiently checkable.

K. Anita Davamani, Assistant Professor, Department of Computer Science and Engineering, BIST, BIHER, Bharath Institute of Higher Education & Research, Selaiyur, Chennai. E-mail: anitadavamani@gmail.com

S. Amudha, Assistant Professor, Department of Computer Science and Engineering, BIST, BIHER, Bharath Institute of Higher Education & Research, Selaiyur, Chennai. E-mail: amudha17s@gmail.com

3. Flexible: In data publishing, the data owner often considered tradeoff between disclosure risk and data utility. A practical privacy criterion should provide this flexibility.
4. External knowledge: The privacy criterion should guarantee safety in the presence of common types of external knowledge.
5. Value-centric: Often, different sensitive values have different degrees of sensitivity (e.g., AIDS is more sensitive than flu).

Thus, a practical privacy criterion should have the flexibility to provide different levels of protection for different sensitive values, not just uniform protection for all the values in the sensitive attribute. We call the latter attribute-centric. An attribute-centric criterion tends to over-protect the data. For example, to protect individuals having AIDS, the data owner must set the strongest level of protection, which is not necessary for individuals having flu. Instead, we take the more flexible value-centric approach. 6. Set-valued sensitive attributes: In many real-world scenarios, an individual may have several sensitive values, e.g., diseases. No existing privacy criterion fully satisfies our desiderata. The most closely-related work is that of Martin et al. While groundbreaking in the treatment of external knowledge, the approach has several important

Shortcomings

- The knowledge quantification is not intuitive. It is hard to understand the practical meaning of k-implications.
- Martin et al. showed that their language can express any logic-based expression of external knowledge, when the number k of basic implications is unbounded. However, their language cannot practically express some important types of knowledge, e.g., simply Flu ∈ Bob[S] (a very common kind of knowledge that the adversary may obtain from a similar dataset). Expressing such knowledge in their language requires (|S|−1) basic implications, where |S| is the number of sensitive values. However, with this number of basic implications, no release candidate can possibly be safe. Thus, Flu ∈Bob[S] will never be used in their criterion.
- The privacy criterion is attribute-centric, and there is no straightforward extension of the proposed algorithm to the more flexible value-centric case. The reason is that the algorithm can only compute max {Pr(s ∈t[S] | K, D*)} for the sensitive value that is most frequent in at least one QI-group. However, the sensitive values that need the most protection (e.g., AIDS) are usually infrequent ones.
- Each individual is assumed to have only one sensitive value. Our work builds upon and addresses the above issues. Note that our language can express some knowledge (e.g., Flu∈ Bob[S]) that cannot be practically expressed in their language, and vice versa.

DISCUSSIONS

The earlier section demonstrated the viability of our approach using an example with eight potentially identifying attributes. In general, the size of the solution space depends on the number of such attributes and the granularity at which they need to be considered. Determining which attributes should be considered as potentially identifying is based on an assessment of possible links to other avail-able data. This needs to be done with typical databases in each domain (e.g., retail). Clearly, as the number of potentially identifying attributes grows, identity disclosure risk in-creases. The corresponding increase in the number of unique combinations of potentially identifying values will have an impact on the k-anonymity approach. Also, the complex-it y of the optimization problem increases due to the larger solution space to be searched. Further experiments are needed to investigate the applicability of this approach to wider data sets. In each domain, in addition to the identifying attributes one needs to determine the sensitive attributes. It has been suggested that sensitive attributes be removed completely from data sets being publicly released [19].

Further work is needed to determine adequate ways of handling these at-tributes if they are included. Clearly, they cannot be targets of predictive modeling using our methods since that will result in their inferential disclosure. This is because the optimization we perform for predictive modeling would group together rows with similar values for the target attribute. This optimization improves the model accuracy while satisfying the identity disclosure constraint, but it also increases the inferential attribute disclosure for the sensitive attribute being targeted. While this is an explicit issue with the k-anonymity approach to anonymization, further investigation is needed on issues related to the inferential disclosure of sensitive attributes even for other approaches (e.g., additive noise and swapping). In many cases only a sample of the data is released. The privacy protection due to sampling has been considered in various works (e.g., [6, 16, 3]). Applying the k-anonymity approach to the release of a sample opens up some new issues. One approach could be to require that the released sample satisfy the k-anonymity requirement.

The choice of k would have to be made taking into account the sampling etc. Alternatively, the k-anonymity requirement could be rest applied to the entire population before a sample of the transformed table is released. The sizes of the groups in the released sample will depend on the form of sampling used (e.g., random, startled). Further work is needed to explore the k-anonymity approach in the context of sampling. For predictive modeling usage the metrics denned in consider predictability using only the potentially identifying attributes. This was done independent of the predictive capabilities of the other non-identifying attributes. Considering both identifying and non-identifying attributes during the data transformation process could lead to better solutions.

Finding an effective way of doing this with potentially large numbers of non-identifying attributes needs further exploration.

Probabilistic Model

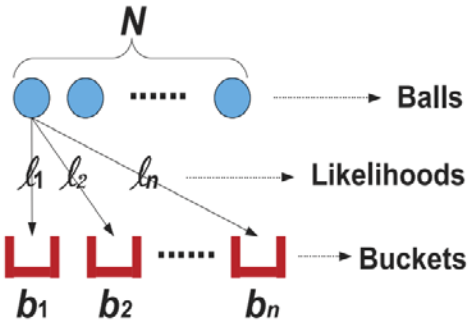

Fig. 1: Model Diagram

A fast algorithm for distributed association rule mining is given in Cheung et. al. [2]. Their procedure for fast distributed mining of association rules (FDM) is summarized below.

1. Candidate Sets Generation: Generate candidate sets CGi(k) based on GLi(k−1), item sets that are supported by the Si at the (k-1)th iteration, using the classic a-priori candidate generation algorithm. Each site generates candidates based on the intersection of globally large (k-1) item sets and locally large (k-1) item sets.
2. Local Pruning: For each X ∈ CGi(k), scan the database DBi at Si to compute X.supi. If X is locally large Si, it is included in the LL i(k) set. It is clear that if X is supported globally, it will be supported in one site.
3. Support Count Exchange: LL i(k) are broadcast, and each site computes the local support for the items in ∪i LL i(k) .
4. Broadcast Mining Results: Each site broadcasts the local support for item sets in ∪i LL i(k) . From this, each site is able to compute L (k)

CONCLUSIONS

Most SMC protocols are expensive in both communication and computation. We introduced a look-ahead approach for SMC protocols that helps involved parties to decide whether the protocol will meet the expectations before initiating it. We presented a look-ahead protocol specifically for the distributed k-anonymity by approximating the probability that the output of the SMC will be more utilized than their local anonymizations. Experiments on real data showed the effectiveness of the approach. Designing look aheads for other SMC protocols stands as a future work. A wide variety of SMC protocols have been proposed especially for privacy preserving data mining applications [12], [17], [28] each requiring a unique look-ahead approach. As for the look-ahead process on distributed anonymization protocols, definitions of k-anonymity definitions can be revisited, more efficient techniques can be developed and experimentally evaluated.

REFERENCES

[1] Das, J., Das, M. P., & Velusamy, P. (2013). Sesbania grandiflora leaf extract mediated green synthesis of antibacterial silver nanoparticles against selected human pathogens. *Spectrochimica Acta Part A: Molecular and Biomolecular Spectroscopy*, *104*, 265-270.

[2] Umanath, K.P.S.S.K., Palanikumar, K., & Selvamani, S. T. (2013). Analysis of dry sliding wear behaviour of Al6061/SiC/Al2O3 hybrid metal matrix composites. *Composites Part B: Engineering*, *53*, 159-168.

[3] Udayakumar, R., Khanaa, V., Saravanan, T., & Saritha, G. (1786). Cross layer optimization for wireless network (WIMAX). *Middle-East Journal of Scientific Research*, *16*(12), 1786-1789.

[4] Kumaravel, A., & Rangarajan, K. (2013). Algorithm for automaton specification for exploring dynamic labyrinths. *Indian Journal of Science and Technology*, *6*(5S), 4554-4559.

[5] Pieger, S., Salman, A., & Bidra, A.S. (2014). Clinical outcomes of lithium disilicate single crowns and partial fixed dental prostheses: a systematic review. *The Journal of prosthetic dentistry*, *112*(1), 22-30.

[6] Vijayaraghavan, K., Nalini, S.K., Prakash, N.U., & Madhankumar, D. (2012). One step green synthesis of silver nano/microparticles using extracts of Trachyspermum ammi and Papaver somniferum. *Colloids and Surfaces B: Biointerfaces*, *94*, 114-117.

[7] Khanaa, V., Mohanta, K., & Satheesh, B. (2013). Comparative study of uwb communications over fiber using direct and external modulations. *Indian Journal of Science and Technology*, *6*(6), 4845-4847.

[8] Khanaa, V., Thooyamani, K. P., & Udayakumar, R. (1798). Cognitive radio based network for ISM band real time embedded system. *Middle-East Journal of Scientific Research*, *16*(12), 1798-1800.

[9] Vijayaraghavan, K., Nalini, S.K., Prakash, N.U., & Madhankumar, D. (2012). Biomimetic synthesis of silver nanoparticles by aqueous extract of Syzygium aromaticum. *Materials Letters*, *75*, 33-35

[10] Caroline, M.L., Sankar, R., Indirani, R.M., & Vasudevan, S. (2009). Growth, optical, thermal and dielectric studies of an amino acid organic nonlinear optical material: l-Alanine. *Materials Chemistry and Physics*, *114*(1), 490-494.

[11] Kumaravel, A., & Pradeepa, R. (2013). Efficient molecule reduction for drug design by intelligent search methods. *International Journal of Pharma and Bio Sciences*, *4*(2), B1023-B1029.

[12] Kaviyarasu, K., Manikandan, E., Kennedy, J., Jayachandran, M., Ladchumananandasiivam, R., De Gomes, U. U., & Maaza, M. (2016). Synthesis and characterization studies of NiO nanorods for enhancing solar cell efficiency using photon upconversion materials. *Ceramics International*, *42*(7), 8385-8394.

[13] Sengottuvel, P., Satishkumar, S., & Dinakaran, D. (2013). Optimization of multiple characteristics of EDM parameters based on desirability approach and fuzzy modeling. *Procedia Engineering*, *64*, 1069-1078.

[14] Anbuselvi S., Chellaram, C., Jonesh S., Jayanthi L., & Edward J.K.P. (2009). Bioactive potential of coral associated gastropod, Trochus tentorium of Gulf of Mannar, Southeastern India. *J. Med. Sci,* 9(5), 240-244.

[15] Kaviyarasu, K., Ayeshamariam, A., Manikandan, E., Kennedy, J., Ladchumananandasivam, R., Gomes, U. U., & Maaza, M. (2016). Solution processing of CuSe quantum dots: Photocatalytic activity under RhB for UV and visible-light solar irradiation. *Materials Science and Engineering: B*, *210*, 1-9.

[16] Kumaravel, A., & Udayakumar, R. (2013). Web portal visits patterns predicted by intuitionistic fuzzy approach. *Indian Journal of Science and Technology*, *6*(5S), 4549-4553.

[17] Srinivasan, V., & Saravanan, T. (2013). Reformation and market design of power sector. *Middle-East Journal of Scientific Research*, *16*(12), 1763-1767.

[18] Kaviyarasu, K., Manikandan, E., Kennedy, J., & Maaza, M. (2015). A comparative study on the morphological features of highly ordered MgO: AgO nanocube arrays prepared via a hydrothermal method. *RSC Advances*, *5*(100), 82421-82428.

[19] Kumaravel, A., & Udhayakumarapandian, D. (2013). Consruction of meta classifiers for apple scab infections. *International Journal of Pharma and Bio Sciences*, *4*(4), B1207-B1213.

[20] Sankari, S. L., Masthan, K. M. K., Babu, N. A., Bhattacharjee, T., & Elumalai, M. (2012). Apoptosis in cancer-an update. *Asian Pacific journal of cancer prevention*, *13*(10), 4873-4878

[21] Harish, B. N., & Menezes, G. A. (2011). Antimicrobial resistance in typhoidal salmonellae. *Indian journal of medical microbiology*, *29*(3), 223-229.

[22] Manikandan, A., Manikandan, E., Meenatchi, B., Vadivel, S., Jaganathan, S. K., Ladchumananandasivam, R., & Aanand, J. S. (2017). Rare earth element (REE) lanthanum doped zinc oxide (La: ZnO) nanomaterials: synthesis structural optical and antibacterial studies. *Journal of Alloys and Compounds*, *723*, 1155-1161.

[23] Caroline, M. L., & Vasudevan, S. (2008). Growth and characterization of an organic nonlinear optical material: L-alanine alaninium nitrate. *Materials Letters*, *62*(15), 2245-2248.

[24] Saravanan T., Srinivasan V., Udayakumar R. (2013). A approach for visualization of atherosclerosis in coronary artery, Middle - East Journal of Scientific Research, 18(12), 1713-1717.

[25] Poongothai, S., Ilavarasan, R., & Karrunakaran, C.M. (2010). Simultaneous and accurate determination of vitamins B1, B6, B12 and alpha-lipoic acid in multivitamin capsule by reverse-phase high performance liquid chromatographic method. *International Journal of Pharmacy and Pharmaceutical Sciences*, *2*(4), 133-139.

[26] Udayakumar, R., Khanaa, V., & Saravanan, T. (2013). Synthesis and structural characterization of thin films of SnO 2 prepared by spray pyrolysis technique. *Indian Journal of Science and Technology*, *6*(6), 4754-4757

[27] Anbazhagan, R., Satheesh, B., & Gopalakrishnan, K. (2013). Mathematical modeling and simulation of modern cars in the role of stability analysis. *Indian Journal of Science and Technology*, *6*(5S), 4633-4641.

[28] Caroline, M.L., & Vasudevan, S. (2009). Growth and characterization of bis thiourea cadmium iodide: A semiorganic single crystal. *Materials Chemistry and Physics*, *113*(2-3), 670-674.

[29] Sharmila, S., Jeyanthi Rebecca, L., & Das, M. P. (2012). Production of Biodiesel from Chaetomorpha antennina and Gracilaria corticata. *Journal of Chemical and Pharmaceutical Research*, *4*(11), 4870-4874.

[30] Dr.Mummoorthy, A., Bhasker, B., & Karthik Deep Yadav, S.J. (2018). Query Formulation Technique Using of Data Web Mining. *Bonfring International Journal of Networking Technologies and Applications, 5*(1), 6-8.

[31] Luigi, and Benjamin, C.(2017). Particle Swarm Optimization (PSO) based Algorithm for the Optimal Location and Setting of FACTS Devices to Improve Voltage Stability. *Bonfring International Journal of Power Systems and Integrated Circuits, 7*(1), 13-18.

[32] Naveen Kumar, B.S., Kumar Raja, D.R., & Olive Esther Kumar (2014). User Behavior Mining in Software as a Service Environment. *International Scientific Journal on Science Engineering & Technology, 17*(5), 537-541.

[33] Dr.Anitha, D. (2018). Analysis of Emergency Communication Networks for Disaster Management. *Journal of Computational Information Systems, 14*(4), 76 - 84.

[34] James, I.S.P. (2013). Face Image Retrieval with HSV Color Space using Clustering Techniques. *The SIJ Transactions on Advances in Space Research & Earth Exploration, 1*(1), 21-24.

[35] Dr.Ponnusamy, S., Omar, M.B., Alshunaybir, F., Alanazi, M., & Alzebak, M. (2018). Fit for Life: Home Personal Coach. *Bonfring International Journal of Software Engineering and Soft Computing, 8*(2), 7-10.

[36] Pazmiño, J.E., & da Silva Rodrigues, C.K.(2015).Simply Dividing a Bitcoin Network Node may Reduce Transaction Verification Time. *The SIJ Transactions on Computer Networks & Communication Engineering (CNCE), 3*(1), 1-5.

[37] Borhan, M.N. (2019). Design of the High Speed and Reliable Source Coupled Logic Multiplexer, *Journal of VLSI Circuits And Systems*, *1*(1), 18-22.

[38] Nandeesh, M.D., & Dr. Meenakshi, M. (2015). Image Fusion Algorithms for Medical Images-A Comparison. *Bonfring International Journal of Advances in Image Processing, 5*(3), 23-26.

[39] Sunitha, G., & Dr.Geethanjali, N. (2018). Heart Disease Detection Using Differential Evolution in Fuzzy Neural Network (DEFNN).. *Journal of Computational Information Systems, 14*(3), 70 - 79.

[40] Thooyamani, K.P., Khanaa, V., & Udayakumar, R. (2013). An integrated agent system for e-mail coordination using jade. *Indian Journal of Science and Technology*, *6*(6), 4758-4761.

[41] Caroline, M. L., Kandasamy, A., Mohan, R., & Vasudevan, S. (2009). Growth and characterization of dichlorobis l-proline Zn (II): A semiorganic nonlinear optical single crystal. *Journal of Crystal Growth*, *311*(4), 1161-1165.

[42] Caroline, M.L., & Vasudevan, S. (2009). Growth and characterization of L-phenylalanine nitric acid, a new organic nonlinear optical material. *Materials Letters*, *63*(1), 41-44.

[43] Kaviyarasu, K., Xolile Fuku, Genene T. Mola, E. Manikandan, J. Kennedy, and M. Maaza. Photoluminescence of well-aligned ZnO doped CeO2 nanoplatelets by a solvothermal route. *Materials Letters*, *183*(2016), 351-354.

[44] Saravanan, T., & Saritha, G. (2013). Buck converter with a variable number of predictive current distributing method. *Indian Journal of Science and Technology*, *6*(5S), 4583-4588.

[45] Parthasarathy, R., Ilavarasan, R., & Karrunakaran, C. M. (2009). Antidiabetic activity of Thespesia Populnea bark and leaf extract against streptozotocin induced diabetic rats. *International Journal of PharmTech Research*, *1*(4), 1069-1072.

[46] Hanirex, D. K., & Kaliyamurthie, K. P. (2013). Multi-classification approach for detecting thyroid attacks. *International Journal of Pharma and Bio Sciences,* 4(3), B1246-B1251

[47] Kandasamy, A., Mohan, R., Lydia Caroline, M., & Vasudevan, S. (2008). Nucleation kinetics, growth, solubility and dielectric studies of L-proline cadmium chloride monohydrate semi organic nonlinear optical single crystal. *Crystal Research and Technology: Journal of Experimental and Industrial Crystallography*, *43*(2), 186-192.

[48] Srinivasan, V., Saravanan, T., Udayakumar, R., & Saritha, G. (2013). Specific absorption rate in the cell phone user's head. *Middle-East Journal of Scientific Research*, *16*(12), 1748-50.

[49] Udayakumar R., Khanaa V., & Saravanan T. (2013). Chromatic dispersion compensation in optical fiber communication system and its simulation, Indian Journal of Science and Technology, 6(6), 4762-4766.

[50] Vijayaragavan, S.P., Karthik, B., Kiran, T.V.U., & Sundar Raj, M. (1990). Robotic surveillance for patient care in hospitals. *Middle-East Journal of Scientific Research*, *16*(12), 1820-1824.