Privacy preserving data mining on partially joint database into mining an association rule

[1]Ms.C.Mahalakshmi, [2]Ms.R.Muthamizharasi, [3]Ms.S.R.Vinotha

[1,2]Student, [3]Assistant Professor
Computer Science and Engineering
Government College Of Engineering, Srirangam, Trichy, India

***Abstract*---Association rule mining and frequent item set mining are two popular and widely studied data analysis techniques for a range of applications. In this paper, we focus on privacy-preserving mining on vertically partitioned databases. In such a scenario, data owners wish to learn the association rules or frequent item sets from a collective data set and disclose as little information about their (sensitive) raw data as possible to other data owners and third parties. To ensure data privacy, we design an efficient homomorphism encryption scheme and a secure comparison scheme. We then propose a cloud-aided frequent item set mining solution, which is used to build an association rule mining solution. Our solutions are designed for outsourced databases that allow multiple data owners to efficiently share their data securely without compromising on data privacy. Our solutions leak less information about the raw data than most existing solutions. In comparison to the only known solution achieving a similar privacy level as our proposed Solutions, the performance of our proposed solutions is three to five orders of magnitude higher. Based on our experiment findings using different parameters and data sets, we demonstrate that the run time in each of our solutions is only one order higher than that in the best non-privacy-preserving data mining algorithms. Since both data and computing work are outsourced to the cloud servers, the resource consumption at the data owner end is very low.**

***KeyWords*---Association rule mining, frequent item set mining, homomorphic encryption scheme**

I. INTRODUCTION

Information forensics and security covers the science,technologies and application. It is to give a combined locus for archival study of basic contributions and mathematics behind information forensics, information safety measures, observation and system applications that incorporate these features. It is specialized field in computer networking that involves securing a computer infrastructure. It is consist of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network accessible resources. It is involves authorization of access to data in a network, which is controlled by the network administrator.

The paper is structured as follows; section 3 provides a Related work of our proposed scheme, Existing system is described in section 4, Proposed system in section 5, followed by the conclusion in section 6.

II. LITERATURE REVIEW

Prof. F. Giannotti, L. V. S. Lakshmanan, A. Monreale, D. Pedreschi, and H. Wang, "Privacy-preserving mining of association rules from outsourced transaction databases," IEEE Syst. J., vol. 7, no. 3, pp. 385–395,Sep. 2013. Spurred by developments such as cloud computing, there has been considerable recent interest in the paradigm of data mining-as-service. A company (data owner) lacking in expertise or computational resources can outsource its mining needs to a third party service provider (server). However, both the items and the association rules of the outsourced database are considered private property of the corporation (data owner). To protect corporate privacy, the data owner transforms its data and ships it to the server, sends mining queries to the server, and recovers the true patterns from the extracted patterns received from the server. In this paper, we study the problem of outsourcing the association rule mining task within a corporate privacy-preserving framework. This paper using the techniques is Outsourced Transaction Databases. It is we empirically assess our encryption method with respect to a real-life transaction database donated by Coop, a cooperative of consumers that is today the largest supermarket chain in Italy.

Prof. B. Dong, R. Liu, and H. Wang, "Result integrity verification of outsourced frequent item set mining," in Proc. 27th Annu. IFIP WG Conf.Data Appl. Secure Privacy (DBSec), Newark, NJ, USA, Jul.2013,pp.258265.[Online].Available:http://dx.doi.org/10.1007/978-3-642-39256-6_17.The data-mining-as-a-service (DMaS) paradigm enables the data owner (client) that lacks expertise or computational resources to outsource its mining tasks to a third-party service provider (server). Outsourcing, however, raises a serious security issue: how can the client of weak computational power verify that the server returned correct mining result. This paper using the two type of techniques. One type is frequent item set mining. It is Frequent item set mining, an important data mining problem, as the main outsourced data mining service. We aim to address the particular problem of verifying whether

the server has returned correct and complete frequent item sets. Other type is Result Integrity Verification. It is One of the main security issues is the integrity of the mining result. There are many possible reasons for the service provider to return incorrect answers. For instance, the service provider would like to improve its revenue by computing with less resource while charging for more. Therefore, it is important to provide efficient mechanisms to verify the result integrity of outsourced data mining computations.

Prof. P. Fournier-Viger, A. Gomariz, T. Gueniche, A. Soltani, C. W. Wu, and V. S. Tseng, "SPMF: A Java open-source pattern mining library," J.Mach. Learn. Res., vol. 15, no. 1, pp. 3389–3393, 2014. Present SPMF, an open-source data mining library offering implementations of more than 55 data mining algorithms. SPMF is a cross-platform library implemented in Java, specialized for discovering patterns in transaction and sequence databases such as frequent item sets, association rules and sequential patterns. The source code can be integrated in other Java programs. Moreover, SPMF offers a command line interface and a simple graphical interface for quick testing. This paper using SPMF technique. It is nothing but SPMF is implemented in Java and is cross-platform. The only requirement to run SPMF is to have Java 7 or higher installed. There are two versions of SPMF. The source code version offers all algorithms from SPMF. The documentation provides an example of how to run each algorithm. It explains the input and output of each algorithm, its main characteristics and where to obtain more information about the algorithm.

Prof. C. Dong and L. Chen, "A fast secure dot product protocol with application to privacy preserving association rule mining", in Proc. 18th Pacific-Asia Conf. Adv. Knowl. Discovery Data Mining(PAKDD),Tainan,Taiwan,May2014,pp.606617.[Online].Available:http://dx.doi.org/10.1007/978-3-319-06608-0_50. Data mining often causes privacy concerns. To ease the concerns, various privacy preserving data mining techniques have been proposed. However, those techniques are often too computationally intensive to be deployed in practice. Efficiency becomes a major challenge in privacy preserving data mining. In this paper we present an efficient secure dot product protocol and show its application in privacy preserving association rule mining, one of the most widely used data mining techniques. This paper using the technique is Privacy Preserving Association Rule Mining. The computation model we consider is two parties each holds part of the transaction set that is vertically partitioned, i.e. one party holds some attributes and the other party holds the rest attributes. In, a secure algorithm for finding association rules on vertically partitioned data was proposed. The Algorithm is a straightforward extension of the Apriori algorithm.

Prof. J. Lai, Y. Li, R. H. Deng, J. Weng, C. Guan, and Q. Yan, "Towards semantically secure outsourcing of association rule mining on categorical data," Inf. Sci., vol. 267, pp. 267–286, May 2014. When outsourcing association rule mining to cloud, it is critical for data owners to protect both sensitive raw data and valuable mining results from being snooped at cloud servers. Previous solutions addressing this concern add random noise to the raw data and/or encrypt the raw data with a substitution mapping. However, these solutions do not provide semantic security; partial information about raw data or mining results can be potentially discovered by an adversary at cloud servers under a reasonable assumption that the adversary knows some plaintext–cipher text pairs. In this paper, we propose the first semantically secure solution for outsourcing association rule mining with both data privacy and mining privacy. This paper using the technique is Outsourcing association rule mining. It is In general, a system of outsourcing association rule mining consists of four algorithms: System Setup, AddEncTransRecord, RetrieveTransRecord and GetFreqItemSets. First of all, data Owner runs algorithm System Setup to output public parameters and a secret key for himself. Then, data Owner executes algorithm AddEncTransRecord to encrypt transaction records before outsourcing data to a cloud server. Algorithm RetrieveTransRecord is dedicated to the convenience of data owner to retrieve transaction records from their encrypted forms.

III. RELATED WORK

A. Privacy-Preserving Association Rule Mining and Frequent Item set Mining on Vertically Partitioned Databases

In [9], the first work to identify and address privacy issues in vertically partitioned databases, a secure scalar product protocol is presented and used to build a privacy-preserving frequent item set mining solution. Association rules can then be found given frequent itemsets and their supports. Since the publication of this seminal work, a number of privacy- preserving association rule mining or frequent item set mining solutions have been published in the literature (see [11]–[13], [28]–[31]).

The most relevant work is the privacy-preserving association rule mining solution presented in [11]. In this solution, a data owner known as the master is responsible for the mining. The other data owners (known as slaves) insert fictitious transactions to their respective datasets, and send the datasets to the master. Each data owner will also send his set of real transactions' IDs to a semi-trusted third-party server. The third-party server is assumed not to be colluding with any data owner, but it cannot be trusted to hold the raw data. The master generates association rule candidates from the joint database containing fictitious data. For each rule candidate $X \Rightarrow Y$, the master sends the ID lists of the transactions containing $X \cup Y$ and the transactions containing X to the third-party server. The server verifies if the rule is qualified or not. Similar to our solutions, a semi-trusted third-party is utilized for the mining. However, unlike our solutions, a data owner (i.e. the master) does the majority of the computational work. Therefore, we can hardly say that such a solution is an outsourced mining solution. Though fictitious data are added in datasets to lower data usability, the master is able to learn significant information about other data owners' raw data from the received datasets. In contrast, our solutions do not leak such information as we do not rely on one particular data owner to undertake the computations and we also encrypt the datasets.

All existing solutions, with the exception of [11], do not utilize a third-party server to server to compute the mining result. Some solutions [12], [13] use asymmetric encryption to compute the supports of itemsets, while other solutions [9], [28]–[30] use a secure scalar product protocol, a set intersection cardinality protocol or a secret sharing scheme to perform these computations. A majority of these solutions expose exact supports to all data owners, resulting in the leakage of information about the data owners' raw data [11]. The only exception is one of [13]'s solutions. In [13], there are two privacy-preserving solutions for frequent item set mining. The first solution exposes exact supports, which is not desirable. The second solution does not expose exact supports. However, association rules cannot be mined based on the result of second solution because confidences cannot be computed without the exact supports. In addition, this solution's method cannot be used to mine association rules because securely computing confidence is more complicated than computing support. In comparison with this solution, our frequent itemset mining solution's computational complexity is significantly lower. Our solutions do not expose exact supports or confidences to data owners. Different from existing solutions based on homomorphic encryption, we use symmetric homomorphic encryption instead of asymmetric homomorphic encryption, and the manner in which we use homomorphic encryption also differs from existing solutions. In our approach, we use homomorphic encryption to create ERVs and build our secure outsourced comparison scheme.

B.Privacy-Preserving Outsourced Association Rule Mining and Frequent Item set Mining

Privacy-preserving outsourced frequent item set mining and association rule mining have been studied in the setting of a single data owner [16],[19]–[21]. In existing solutions, the data owner outsources their data and the mining task to the cloud, but at the same time, wish to keep the raw data secret from the cloud. Generally, data items in the database are encrypted using a substitution cipher prior to outsourcing. Reference [19] proposed a solution to counter frequency analysis attack on substitution cipher. However, a later work [20] demonstrated that [19]'s solution is not secure. Giannotti et al. proposed a solution based on k-anonymity frequency [16], [21]. To counter frequency analysis attack, the data owner inserts fictitious transactions in the encrypted database to conceal the item frequency. After inserting the fictitious transactions, any item in the encrypted database will share the same frequency with at least $k - 1$ other items. The data owner sends the encrypted database of both the real and fictitious transactions to the cloud. The cloud runs a classic frequent item set mining algorithm, and returns the result (frequent itemsets and their supports) to the data owner. The data owner revises these itemsets' supports by subtracting them with these itemsets' corresponding occurrence counts in the fictitious transactions respectively. Finally, the data owner decrypts the received itemsets with the revised supports higher than the frequency threshold, and generates association rules based on found frequent itemsets. Our solutions use their techniques to conceal the raw data from the cloud and mitigate frequency analysis attack that can be undertaken by the cloud. Using these techniques alone, however, is not sufficient to protect data privacy in the vertically partitioned database setting. To cancel out fictitious transactions, both [21] and [16] require the data owner to count itemset occurrences in fictitious transactions. In the vertically partitioned database setting, data owners are unable to perform such calculation using the techniques described in [21] and [16]. In our solutions, the cloud rather than the data owners cancels out fictitious transactions in a privacy-preserving manner, and the under- lying techniques are our homomorphic encryption, secure comparison and ciphertext tag schemes.

Another recent work [32] proposed a privacy-preserving outsourced association rule mining solution based on predicate encryption. This solution is resilient to chosen-plaintext attacks on encrypted items, but it is vulnerable to frequency analysis attacks. Applying this solution to vertically partitioned databases will also result in the leakage of the exact supports to data owners. In this paper, our adversary model is different. We assume the cloud has knowledge of the item frequencies instead of chosen plaintext-ciphertext pairs, and our solutions are resilient to frequency analysis attacks.

C.Other Related Work

Other than the settings of vertically partitioned databases and cloud/third-party-aided mining, privacy-preserving frequent itemset mining and association rule mining have been studied in the settings of horizontally partitioned databases [10], [33]–[35], data publishing [36] and differential privacy [37]. These settings are beyond the scope of this paper.

IV. EXISTING SYSTEM

The most relevant work is the privacy-preserving association rule mining solution presented. In this solution, a data owner known as the master is responsible for the mining. The other data owners (known as slaves) insert fictitious transactions to their respective datasets, and send the datasets to the master. Each data owner will also send his set of real transactions' IDs to a semi-trusted third-party server. The data owner sends the encrypted database of both the real and fictitious transactions to the cloud. The cloud runs a classic frequent item set mining algorithm, and returns the result (frequent item sets and their supports) to the data owner. The data owner revises these item sets' supports by subtracting them with these item sets' corresponding occurrence counts in the fictitious transactions respectively. Finally, the data owner decrypts the received item sets with the revised supports higher than the frequency threshold, and generates association rules based on found frequent item sets.

Disadvantages

- Encryption and decryption problems occurs using asymmetric key.
- Duplicate records are executed during transaction.
- Complex problems occur.
- Unauthorized data owners can be accessed.

- Only limited amount of storage.

V. PROPOSED SYSTEM

Privacy-preserving outsourced frequent item set mining solution for vertically partitioned databases and also horizontally partitioned databases. The user access any type of database in our convenient. This allows the data owners to outsource mining task on their joint data in a privacy-preserving manner. Our solutions also ensure the privacy of the mining results from the cloud. Compared with most existing solutions, our solutions leak less information about the data owners' raw data. We focus on privacy-preserving mining on vertically and horizontally partitioned databases. In such a scenario, data owners wish to learn the association rules or frequent item sets from a collective data set and disclose as little information about their (sensitive) raw data as possible to other data owners and third parties. To ensure data privacy, we design an efficient homomorphic encryption scheme and a secure comparison scheme. The data owners are not willing to send their raw data to a central site due to privacy concerns. If each data owner has one or more rows (i.e. transactions) in the joint database, we say that the database is horizontally partitioned.

Advantages

- Efficient homomorphism encryption scheme
- To ensure data privacy.
- Multiple data owners efficiently to share their data securely.
- Store unlimited amount of data.
- To simplify columns and rows.
- Without fictitious transaction.
- Only authorized data owners can be accessed.

Architecture Diagram

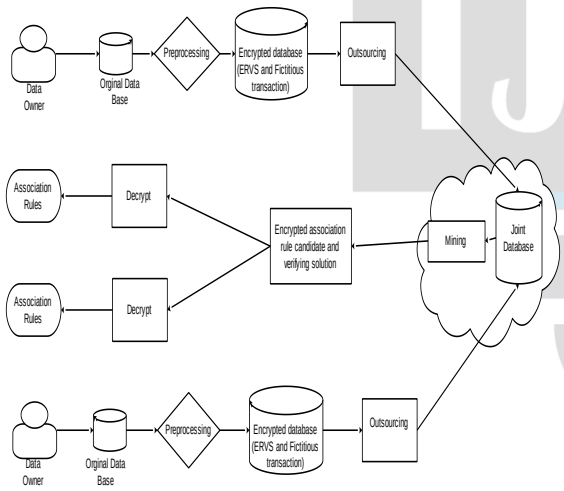

Fig.1 System Architecture diagram

System Modules

The system comprises of the following modules which include,

- Data Owner
- Privacy Preserving and outsourcing with fictitious transaction
- Vertical and horizontal partitioned database
- Association Rule mining

Data Owner

The data owner has own private database. The database contains transaction values which are the real transaction of product selling details. Then the data owners add the fictitious transaction to improve the rating of the product for non selling items. The data owner analyzes the database then the data owner can add encryption.

Privacy Preserving and Outsourcing with Fictitious Transaction

The data owner has a original data base tense to implement symmetric homomorphic encryption scheme using secrete key to getting more confidential privacy to data owner. The data owner can outsource the database into cloud. The database contains the encrypted realness value and fictitious transaction.

Vertical and horizontal Partitioned Database

Cloud should convert the database into joint database. Several data owners outsourcing their own data bases in encrypted format. The cloud analyzing encrypted databases then convert to the vertically partitioned and horizontal partitioned database. The vertically partitioned databases define on Colum simplification of databases. The horizontal partitioned databases define on row simplification of databases.

Association Rule Mining

When cloud finishing vertically partitioned database and also finding the association rules. The data owner mining association rules from the cloud then decrypt association rules. The data owner can use symmetric homomorphic encryption to decrypt the association rules.

VI. CONCLUSION

In this paper, we proposed a privacy-preserving outsourced frequent item set mining solution for vertical and horizontal partitioned databases. This allows the data owners to outsource mining task on their joint data in a privacy-preserving manner. on this solution, we built a privacy preserving outsourced association rule partitioned databases. Our solutions protect data owner's raw data from other data owners and the cloud. Our solutions also ensure the privacy of the mining results from the cloud. Compared with most existing solutions, our solutions leak less information about the data owners' raw data. Our evaluation has also demonstrated that our solutions are very efficient; therefore, our solutions are suitable to be used by data owners wishing to outsource their databases to the cloud but require a high level of privacy without compromising on performance. To realize our solutions, an efficient homomorphic encryption scheme and a secure outsourced comparison scheme were presented in this paper. Both schemes have potential usage in other secure computation

applications, such as secure data aggregation, beyond the data mining solutions described in this paper. Demonstrating the utility of the proposed homomorphic encryption scheme and outsourced comparison scheme in other settings will be the focus of future research.

REFERENCES

[1] T. Brijs, G. Swinnen, K. Vanhoof, and G. Wets, "Using association rules for product assortment decisions: A case study," in *Proc. SIGKDD*, 1999,pp. 254–260.

[2] S. E. Brossette, A. P. Sprague, J. M. Hardin, K. B. Waites, W. T. Jones,and S. A. Moser, "Association rules and data mining in hospital infection control and publichealth surveillance," *J. Amer. Med. Inform. Assoc*, vol. 5, no. 4, pp. 373–381, 1998.

[3] B. Mobasher, H. Dai, T. Luo, and M. Nakagawa, "Effective personal-ization based on association rule discovery from Web usage data," in *Proc. WIDM*, 2001, pp. 9–15.

[4] C. Creighton and S. Hanash, "Mining gene expression databases for association rules," *Bioinformatics*, vol. 19, no. 1, pp. 79–86, 2003.

[5] X. Yin and J. Han, "CPAR: Classification based on predictive association rules," in *Proc. SIAM SDM*, 2003, pp. 1–5.

[6] R. Agrawal and R. Srikant, "Fast algorithms for mining association rules," in *Proc. VLDB*, 1994, pp. 1–13.

[7] M. J. Zaki, "Scalable algorithms for association mining," *IEEE Trans. Knowl. Data Eng.*, vol. 12, no. 3, pp. 372–390, May/Jun. 2000.

[8] J. Han, J. Pei, and Y. Yin, "Mining frequent patterns without candidate generation," in *Proc. ACM SIGMOD*, pp. 1–12, 2000. *ACM SIGMOD*, pp. 1–12, 2000.

[9] J. Vaidya and C. Clifton, "Privacy preserving association rule mining in vertically partitioned data," in *Proc. SIGKDD*, 2002, pp. 639–644.

[10] M. Kantarcioglu and C. Clifton, "Privacy-preserving distributed mining of association rules on horizontally partitioned data," *IEEE Trans. Knowl. Data Eng.*, vol. 16, no. 9, pp. 1026–1037, Sep. 2004.

[11] B. Rozenberg and E. Gudes, "Association rules mining in vertically partitioned databases," *Data Knowl. Eng.*, vol. 59, no. 2, pp. 378–396,2006.

[12] J. Zhan, S. Matwin, and L. Chang, "Privacy-preserving collaborative association rule mining," in *Proc. DBSEC*, 2005, pp. 153–165.

[13] S. Zhong, "Privacy-preserving algorithms for distributed mining of frequent itemsets," *Inf. Sci.*, vol. 177, no. 2, pp. 490–503, 2007.

[14] P. Paillier, "Public-key cryptosystems based on composite degree resid-uosity classes," in *Proc. EUROCRYPT*, 1999, pp. 223–238.

[15] R. Cramer, R. Gennaro, and B. Schoenmakers, "A secure and optimally efficient multi-authority election scheme," *Eur. Trans. Telecommun.*,vol. 8, no. 5, pp. 481–490, 1997.

[16] F. Giannotti, L. V. S. Lakshmanan, A. Monreale, D. Pedreschi, and H. Wang, "Privacy-preserving mining of association rules from out- sourced transaction databases," *IEEE Syst. J.*, vol. 7, no. 3, pp. 385–395, Sep. 2013.

[17] B. Dong, R. Liu, and H. Wang, "Result integrity verification of out- sourced frequent itemset mining," in *Proc. 27th Annu. IFIP WG Conf. Data Appl. Secur. Privacy (DBSec)*, Newark, NJ, USA, Jul. 2013, pp. 258–265. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-39256-6_17.

[18] R. Liu and H. Wang, "Result integrity verification of outsourced privacy-preserving frequent itemset mining," in *Proc. SIAM Int. Conf. Data Mining*, Vancouver, BC, Canada, Apr./May 2015, pp. 244–252. [Online]. Available: http://dx.doi.org/10.1137/1.9781611974010.28

[19] W. K. Wong, D. W. Cheung, E. Hung, B. Kao, and N. Mamoulis, "Security in outsourcing of association rule mining," in *Proc. VLDB*,2007, pp. 111–122.

[20] I. Molloy, N. Li, and T. Li, "On the (in)security and (im)practicality of outsourcing precise association rule mining," in *Proc. ICDM*, Dec. 2009, pp. 872–877.

[21] F. Giannotti, L. V. S. Lakshmanan, A. Monreale, D. Pedreschi, and W. Wang, "Privacy-preserving data mining from outsourced databases,"in *Proc. CPDP*, 2011, pp. 411–426.

[22] *FIPS Publication 180-1: Secure Hash Standard*, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, 1995.

[23] *FIPS Publication 180-2: Secure Hash Standard*, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, 2002.

[24] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469–472, Jul. 1985. [Online]. Available: http://dx.doi.org/10.1109/ TIT.1985.1057074

[25] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, "Efficient algorithms for solving overdefined systems of multivariate polynomial equations," in *Proc. EUROCRYPT*, 2000, pp. 392–407.

[26] P. Fournier-Viger. *Real-life Datasets in SPMF Format*, accessed on Apr. 6, 2016. [Online]. Available: http://www.philippe-fournier-viger.com/spmf/index.php?link=datasets.php

[27] P. Fournier-Viger, A. Gomariz, T. Gueniche, A. Soltani, C. W. Wu, and V. S. Tseng, "SPMF: A Java open-source pattern mining library," *J. Mach. Learn. Res.*, vol. 15, no. 1, pp. 3389–3393, 2014.

[28] J. Vaidya and C. Clifton, "Secure set intersection cardinality with application to association rule mining," *J. Comput. Secur.*, vol. 13, no. 4, pp. 593–622, 2005.

[29] X. Ge, L. Yan, J. Zhu, and W. Shi, "Privacy-preserving distributed association rule mining based on the secret sharing technique," in *Proc.SEDM*, Jun. 2010, pp. 345–350.

[30] R. Kharat, M. Kumbhar, and P. Bhamre, "Efficient privacy preserving distributed association rule mining protocol based on random number," in *Intelligent Computing, Networking, and Informatics*. Raipur, Chhat- tisgarh, India: Springer, 2014, pp. 827–836.

[31] C. Dong and L. Chen, "A fast secure dot product protocol with application to privacy preserving association rule mining," in *Proc. 18th Pacific-Asia Conf. Adv. Knowl. Discovery Data*

Mining (PAKDD), Tainan, Taiwan, May 2014, pp. 606–617. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-06608-0_50

[32] J. Lai, Y. Li, R. H. Deng, J. Weng, C. Guan, and Q. Yan, "Towards semantically secure outsourcing of association rule mining on categorical data," *Inf. Sci.*, vol. 267, pp. 267–286, May 2014.

[33] T. Fukasawa, J. Wang, T. Takata, and M. Miyazaki, "An effective distributed privacy-preserving data mining algorithm," in *Proc. 5th Int. Conf. IDEAL*, 2004, pp. 320–325.

[34] C. Su and K. Sakurai, "A distributed privacy-preserving association rules mining scheme using frequent-pattern tree," in *Proc. ADMA*, 2008,pp. 170–181.

[35] M. G. Kaosar, R. Paulet, and X. Yi, "Secure two-party association rule mining," in *Proc. ACSW-AISC*, 2011, pp. 15–22.

[36] J.-L. Lin and J. Y.-C. Liu, "Privacy preserving itemset mining through fake transactions," in *Proc. ACM Symp. Appl. Comput. (SAC)*, Seoul, South Korea, Mar. 2007, pp. 375–379. [Online]. Available:http://doi.acm.org/10.1145/1244002.1244092

[37] B. N. Keshavamurthy, A. M. Khan, and D. Toshniwal, "Privacy pre- serving association rule mining over distributed databases using genetic algorithm," *Neural Comput. Appl.*, vol. 22, no. 1, pp. 351–364, 2013.