ISSN 2616-5775 Vol. 7, Issue 5: 207-214, DOI: 10.25236/AJCIS.2024.070527

A Review on Technologies of Secure Outsourced Association Rule Mining in Cloud Computing Environment

Wei Wu[1*], Jialu Hao[2,3], Lifang Bai[1]

[1]*Information Engineering University, Zhengzhou, 450001, China*
[2]*Xi'an Satellite Control Center, Xi'an, 710043, China*
[3]*Henan Key Laboratory of Network Cryptography Technology, Zhengzhou, 450001, China*
**Corresponding author*

Abstract: *With the rapid development of cloud computing technology, more users are now paying attention to secure and efficient outsourced data mining in cloud computing environment. In this paper, focusing on one of the important data mining tasks, we review existing researches on outsourced association rule mining. We mainly consider three aspects, i.e., privacy protection, result verification and access control of outsourced association rule mining, summarizing the corresponding solutions and analyze their deficiencies. Besides, we propose three future research suggestions. In summary, this paper provides theoretical and technical supports to design secure and efficient outsourced association rule mining solutions.*

Keywords: *Cloud-based Secure Outsourcing; Association Rule Mining; Privacy Protection; Result Verification; Access Control*

1. Introduction

With the rapid development of cloud computing technology, cloud service providers provide users with powerful and flexible data storage and computing services. Outsourcing data mining tasks to cloud service providers can significantly reduce users' IT costs and improve operation and maintenance efficiency. However, with the increasing requirements of users on the security of cloud data outsourcing, the verifiability of data mining results, and multi-user access control, how to design a secure and efficient cloud data mining security outsourcing scheme is an important issue that needs to be solved urgently in academia and industry.

For example, a large retailer plans to store its merchandise sales data in the cloud server, and uses the powerful computing power of the cloud to perform data mining tasks to discover hidden high-value information. However, due to the uncontrollability of the cloud, the retailer needs to consider the following three aspects when outsourcing data mining: First, the original data and mining results are of high value and may contain the privacy information of customers, so their security needs to be effectively protected; Second, the cloud server may return the wrong mining results due to execution failure, human error or interest factors, so the mining results need to be effectively verified; Third, based on mutual benefit, the retailer may want to realize the data mining of business partners on their outsourced databases, so it needs to carry out effective access control for multiple authorized users.

In view of this, designing an effective outsourcing scheme for cloud data mining security needs to focus on three aspects: data security, verifiability of data mining results and multi-user access control. The existing research work has explored these problems respectively, but there are still some deficiencies. In terms of cloud data security, researchers mainly use protection methods based on data distortion, data anonymity and data encryption. The methods based on data distortion and data anonymity have weak security and reduce the accuracy of mining results since only the original data is disturbed or anonymized. The method based on data encryption usually uses the expensive public key encryption algorithm to design the encrypted computing protocol, so it has low operational efficiency. In terms of the verifiability of data mining results, researchers mainly use general verifiability computing technology and verification technology for specific data mining algorithms. The general verifiability computing technology has a large computational overhead, so it cannot be applied to the outsourcing data mining scenario with complex computation processes. The other kind of method

ISSN 2616-5775 Vol. 7, Issue 5: 207-214, DOI: 10.25236/AJCIS.2024.070527

mainly uses the scheme of falsified sample implantation for plaintext outsourcing data, which solves the problem of association rule mining, K-means clustering outsourcing and other result verification problems, but it cannot be applied to the application scenario of ciphertext mining outsourcing. In terms of multi-user access control, researchers mainly use role-based access control, attribute-based encryption and other technologies to achieve fine-grained access control, but they cannot support ciphertext computing operations, so they are not applicable to the application scenarios of ciphertext mining outsourcing.

To sum up, research on data mining security outsourcing technology under cloud computing environment has important theoretical value and practical significance, which promotes the development of cloud computing technology. In this paper, we focus on one of the important research directions in the field of data mining outsourcing, i.e., secure association rule mining outsourcing in cloud computing environment. We first review existing research works, summarize the schemes and analyze their deficiencies. Based on these analyses, we propose several promising research directions, which may support solving the problem of secure data mining outsourcing.

The rest of the paper is organized as follows. We discuss the research works on privacy protection of outsourced association rule mining in Section 2. The existing researches on result verification of outsourced cloud data mining are reviewed in Section 3. We summarize the schemes of access control on outsourced cloud data mining in Section 4. The future research suggestions are proposed in Section 5. At last, we conclude the paper in Section 6.

2. Privacy-preserving outsourced association rule mining

In order to realize privacy preserving of outsourced association rules mining in the cloud, researchers first encrypt the data using alternative encryption algorithm, and put forward a series of solutions[1]-[4]. Wong et al. [1] encrypt the original transaction data through mapping function in their scheme, and implant random forgery items in ciphertext transaction data to enhance the security of the scheme. However, in view of the above scheme, Molloy et al.[5] point out that the forgery items can be removed by calculating the low correlation between the items, so that the high-frequency items can be effectively identified.

In order to improve the security of the scheme, Tai et al. [2] introduced k-support anonymity mechanism while using alternative encryption algorithm, so as to ensure that the support of each item is at least similar to that of other k-1 items. Similarly, Giannotti et al. [3] proposed the k-privacy approach in their scheme, which requires each item set to be indistinguishable from other k-1 item sets with the same size, thus enhancing the effect of data privacy protection.

In order to ensure the security and efficiency of the scheme at the same time, Li et al. [4] proposed a symmetric homomorphic encryption algorithm and a secure comparison protocol. They designed a secure outsourcing scheme for association rule mining by combining the replacement encryption algorithm and the cryptographic hash function. Although the scheme has high operational efficiency, it requires the data owner to stay online and participate in the mining process during its execution. In addition, Wang et al. [6] pointed out that the homomorphic encryption algorithm proposed in the above literature [4] is not secure, and the attacker can solve the key if some clear ciphertext pairs are known. Although the above research works [1]-[4] can protect data privacy to a certain extent, none of them can achieve semantic security of ciphertext, so they cannot effectively resist chosen plaintext attacks.

In order to realize the semantic security of ciphertext data, Lai et al. [7] designed a secure outsourcing scheme for association rule mining using predicate encryption algorithm [8] and dual-system encryption method [9]. The scheme effectively protects the privacy of the original data and the mining results, and provides a method to verify the correctness of the mining results. However, because the scheme uses a fixed ciphertext for each item, it cannot effectively resist frequency analysis attacks. In addition, the scheme has a high computational overhead, which reduces its practicality on large databases.

Considering the different requirements of users for data privacy protection, Yi et al. [10] used distributed ElGamal encryption algorithm [11] to design three security outsourcing schemes for association rule mining with different security levels. In this work, the author first uses the Plaintext Equality Test (PET) [12] method to design the first solution, which does not have the true support of the hidden itemset, so it cannot effectively resist the background knowledge attack. By adding the forged transaction data to the ciphertext database, mixing it with the real transaction data using ElGamal re-

ISSN 2616-5775 Vol. 7, Issue 5: 207-214, DOI: 10.25236/AJCIS.2024.070527

encryption and random shuffling, the authors realize the hiding of the itemset support in the second solution. However, this solution cannot completely hide the original transaction data, so the third solution with higher security is proposed to solve this problem. Although this work can better analyze and solve the privacy protection problem in outsourced association rule mining, it requires at least two cloud servers to cooperate in mining, which has a high communication overhead.

By using a fully homomorphic encryption algorithm [13], Liu et al. [14] proposed two secure outsourcing schemes for association rule mining, and used α -pattern uncertainty method to enhance the effect of privacy protection. However, since the cloud server cannot directly compare the homomorphic ciphertext in this scheme, users need to stay online and participate in the calculation during the outsourcing mining process, resulting in additional computing overhead. In addition, each element in the binary transaction matrix is encrypted separately in this scheme, which requires a large computational overhead in the subsequent ciphertext calculation.

In order to improve the efficiency of outsourced mining, Imabayashi et al. [15] designed a secure outsourcing scheme for association rule mining by using BGV homomorphic encryption algorithm [16] and ciphertext packaging technology SIMD (Single Instruction Multiple Data) [17]. By packaging multiple groups of plaintext data into one ciphertext, the scheme realizes efficient parallel operation, thus significantly improving the operation efficiency. However, the scheme also requires the data owner to stay online for decryption and comparison operations, which affects the applicability of the scheme.

Aiming at the secure outsourcing of association rule query, Qiu et al. [18] used two homomorphic encryption algorithms, Paillier [19] and BGN [20], to design three outsourcing schemes with different security requirements. However, similar to other schemes that use public key encryption algorithms, the above schemes require large computational overhead and thus have low operational efficiency. Considering the application requirement of multiple users using different keys, Liu et al. [21] designed a secure outsourcing scheme for association rule query using BCP encryption algorithm [22] with additive homomorphism and double decryption mechanism. However, this scheme assumes that all the query users can obtain the master decryption private key, which causes a large risk of key disclosure and affects the security and practicability of the scheme.Wu et al. [23] proposed an efficient user-offline privacy-preserving frequent itemset query scheme using YASHE [24] and Paillier [19] homomorphic encryptions. This scheme protects transaction database with semantic security, preserves mining privacy and resists frequency analysis attacks. Besides, the scheme is efficient by performing inherent parallel computations using ciphertext packing technique SIMD [17].

Based on the aforementioned analyses, the existing researches on privacy protection of outsourced cloud association rules mining mainly used alternative encryption algorithms, data anonymity mechanisms, symmetric homomorphic encryption algorithms and public key homomorphic encryption algorithms. These schemes are usually unable to meet the realistic requirements of high security, efficiency and accuracy of outsourced cloud association rule mining, or require users to participate in the online computing processes, which affects the practicality of the schemes. Therefore, it is worth to analyze the nature and performance of ciphertext operation using different encryption algorithms. Then, researchers should select appropriate encryption algorithm, design interactive ciphertext secure computing protocol, and build a more secure and efficient privacy protection outsourcing scheme for cloud association rule mining.

3. Result verification of outsourced association rule mining

In the verification of outsourced frequent itemset mining results, the following two requirements should be realized: First, all frequent itemsets returned are true and frequent, and their corresponding support degrees are correct, guaranteeing the correctness of the results; Second, all frequent itemsets are in the returned mining results, that is, to ensure the integrity of the results. Wong et al. [25] proposed a result verification method for outsourced frequent itemset mining. The basic idea is to ensure the correctness and integrity of mining results with a high probability by implanting forged itemsets in the original database. However, this method assumes that the cloud server does not have the relevant background knowledge of the outsourced database, that is, it cannot distinguish between the real itemsets and the forged itemsets. Therefore, it cannot effectively resist the inference attacks based on background knowledge.

In order to resist inference attacks, Dong et al. [26] proposed a method to construct artificial frequent and infrequent itemsets based on real transaction data. They designed a verification scheme for

ISSN 2616-5775 Vol. 7, Issue 5: 207-214, DOI: 10.25236/AJCIS.2024.070527

outsourced frequent itemset mining, which is suitable for large-scale mining outsourcing application scenarios. However, this method requires users to save part of the verification data locally and participate in the calculation process of result verification, which affects the practicability of the scheme. Similarly, Liu et al. [27] designed a probabilistic verification method by constructing artificial frequent and infrequent itemsets, and used data perturbation to achieve a weak privacy-preserving level for outsourced frequent itemset mining.

In order to improve the accuracy of result verification, Dong et al. [28] proposed a method of deterministic result verification based on cryptography. They constructed Merkle hash tree as the data structure of result verification, and designed intersection verification protocol to judge the correctness of returned results. However, the computational efficiency of this method is low. The computational overhead of generating result verification evidence is equivalent to the search space of frequent itemset mining processes. Based on their previous work, Dong et al. [29] enhanced their probabilistic approach and deterministic approach, also designed verification methods for data and mining update circumstances.

Rong et al. [30][31] proposed a verifiable and secure outsourced frequent pattern mining protocol using Shamir's secret sharing scheme by leveraging the redundancy of cloud servers. This solution does not construct fake item or generate cryptographic proofs, which could resist frequency analysis attacks under semi-honest threat model. However, the performance of verification depends on the number of cloud servers, which inevitably requires more cost for the users.

To efficiently verify the results of outsourced frequent itemset mining, Zhang et al. [32] proposed a light-weight metamorphic-based scheme by constructing a set of metamorphic relations, which defines the relation among source and follow-up transaction databases and itemsets. However, this scheme requires extra storage for follow-up datasets, as well as more communication between users and cloud servers. Similarly, Hong et al. [33] proposed a solution to check the frequent itemset mining results by designing five new metamorphic relations, which also introduces more operation costs for the users.

Recently, Zhao et al. [34] introduced Paillier homomorphic encryption to perform privacy-preserving outsourced frequent itemset mining. To verify the mining result, they also added artificial itemsets in the transaction database using the technique proposed in [25], and achieved frequency analysis attack resistance by adopting the algorithm proposed in [3]. Chen et al. [35] used the BLS signature [36] to perform verifiable privacy-preserving association rule mining, which simultaneously achieves security and verification, but also requires more computation overheads.

Based on the above research results, the existing cloud data mining outsourcing results verification schemes mainly adopt artificial itemsets implantation, cryptographic proofs construction, metamorphic-based method, Shamir's secret sharing and BLS signature. These schemes achieved the verification of result correctness and integrity, but still have some shortcomings, such as being unable to efficiently perform verification on encrypted transactions, unable to support the dynamic update of the outsourced database, and have relatively high computation costs on the user side. Therefore, to achieve secure outsourced association rule mining, an efficient verification method for encrypted data mining results should be built, which must support the dynamic update of the outsourced encrypted database and reduce the authentication calculation cost of the user side.

4. Access control of outsourced cloud data mining

With the continuous development of new technologies in the field of cryptography, researchers have proposed a series of ciphertext-based access control schemes, including traditional PKI Based ciphertext access control model, Identity Based Encryption (IBE) based ciphertext access control model, Attribute Based Encryption (ABE) based ciphertext access control model, etc. The basic ideas of these models are similar, while they use different encryption systems in data encryption, key management and distribution.

In the traditional PKI based ciphertext access control model, the data owner first encrypts the data using the symmetric encryption algorithm, then encrypts the symmetric key using the public key of each authorized user, and uploads the encrypted data and encrypted key to the cloud. Then, the authorized user can decrypt the symmetric key using his private key, and then decrypt the plaintext data. However, this method has the following disadvantages: (1) The data owner needs to obtain the public keys of all authorized users and carry out corresponding key encryption, resulting in high computing overhead and key management costs. (2) With the increasing number of authorized users, the storage

ISSN 2616-5775 Vol. 7, Issue 5: 207-214, DOI: 10.25236/AJCIS.2024.070527

cost of cloud key ciphertext will increase significantly; (3) When it is necessary to revoke the user's access right, the data owner needs to re-select the symmetric key, and repeat the encryption and ciphertext upload tasks, which brings great computing and communication costs.

In view of the shortcomings of the ciphertext access control model based on traditional PKI, researchers propose an identity-based ciphertext access control model [37]-[38], which realizes flexible access control by taking the identity of authorized users as their legitimate public keys. In this model, the data owner can encrypt the data directly by using the authorized user's ID, thus reducing the cost of key management and key encryption. However, this model still requires the data owner to manage the list of authorized users and related information, which cannot achieve fine-grained access control requirements.

In order to effectively improve the flexibility of ciphertext access control and further reduce the cost of key management, Sahai and Waters et al. designed a fuzzy identity-based encryption mechanism by introducing the concept of attributes, forming the prototype of attribute-based encryption. After that, researchers divided the attribute-based encryption algorithms into two categories, namely Ciphertext-Policy ABE (CP-ABE) and Key-Policy ABE (KP-ABE), and carried out a lot of research works [39]-[43], which achieve fine-grained access control. In addition, for the research of ABE-based access control, academics have carried out in-depth exploration in the aspects of user permission revocation [44], access policy verifiability [45], ABE decryption outsourcing [46]-[48], etc., which effectively improve the applicability of the scheme and reduce the computing cost of the client.

Based on the above research results, the existing ciphertext access control schemes are mainly applied to the application scenario of cloud storage and achieve fine-grained access control policies. These solutions effectively ensure the security and controllability of cloud ciphertext data, and significantly reduce the computing overhead and key management cost of cloud users. However, the existing ciphertext access control schemes still cannot directly support the needs of cloud outsourced ciphertext computing, and cannot effectively solve the practical problems of multi-user outsourced data mining access control. Therefore, researchers should design secure and efficient ciphertext access control schemes based on the characteristics of specific data mining tasks on outsourced encrypted cloud database.

5. Future research suggestions

By reviewing existing research works, there are still many problems to be solved in the secure outsourcing of association rule mining in the cloud computing environment. Here, we consider three aspects of outsourced data mining, i.e., data security, mining results verification and multi-user access control, and try to provide some future research suggestions.

To improve the privacy protection of outsourced association rule mining, researchers may consider the characteristics of full-homomorphic encryption algorithm and the mechanism of ciphertext parallel computing. Specifically, based on Apriori association rule mining algorithm, combined with the privacy protection requirements of cloud ciphertext data mining, the mining calculation process could be broken down into multiple steps, such as frequent itemset calculation, itemset connection, itemset pruning, strong association rule calculation, mining result decryption. The privacy protection requirements of different steps should be analyzed, and the corresponding secure computing protocol framework should be designed. Next, for the detailed analysis of the computing operations involved in association rule mining, the original data could be encrypted using semantically secure homomorphic encryption algorithm to support basic ciphertext arithmetic operations. It is proposed to use ciphertext packaging technology to package the plaintext data to support efficient parallel ciphertext computing operations. Besides, the non-collusive two-cloud model could be used to design interactive secure computing protocols to support each computing step of ciphertext association rule mining. Finally, considering the overall computing process of outsourced association rule mining, researchers should design interfaces of different secure computing protocols, then combine them into a complete privacy protection scheme of outsourced cloud association rule mining.

To achieve effective result verification of outsourced cloud data mining, researchers may consider the requirement of dynamic update of ciphertext database, as well as the generation and implantation strategy of ciphertext forgeries. Specifically, researchers should first analyze the nature of the forged sample and its influence on the results of association rule mining. They should also figure out the probability of successful result verification after implantation of the forged sample. The construction of the forged samples could be combined with the statistical regularity of frequent itemsets in association

ISSN 2616-5775 Vol. 7, Issue 5: 207-214, DOI: 10.25236/AJCIS.2024.070527

rule mining. The knowledge of graph theory could be used to reduce the computational cost and improve the reliability of the result verification. Next, researchers could analyze the structural characteristics of the ciphertext outsourcing database, find advantages and disadvantages of horizontal and vertical implantation of forged samples in the ciphertext database. Researchers should also consider the influence of different minimum support thresholds and other parameters on the structure and number of forged samples. Based on these analyses, the technology of ciphertext location mask could be used to realize the dynamic update of forged samples. Then, the ciphertext mining results after implantation of forged samples should be analyzed. Finally, researchers could design an efficient verification scheme for the correctness and integrity of outsourced association rule mining results.

To perform efficient access control of outsourced cloud data mining, researchers may consider the requirements of multi-user fine-grained access control by using attribute-based encryption and proxy re-encryption. Specifically, researchers should first analyze the access control requirements of multi-user outsourcing situation, estimate the impact of complex computing operations of access control, and design a fine-grained outsourced association rule mining access control framework. Next, the characteristics of the original ciphertext data and the intermediate calculation results should be analyzed. Then, researchers could use the proxy re-encryption technology to convert the ciphertext, and construct the corresponding proxy re-encryption key generation method, which is utilized to realize the conversion of the ciphertext mining results for specified users. On this basis, the key encapsulation mechanism using attribute-based encryption could be utilized to achieve efficient key management. Finally, using these suggested technologies, researchers could build a fine-grained access control scheme for outsourced cloud association rule mining.

We hope these research suggestions are useful to improve the security, efficiency and verifiableness of outsourced cloud association rule mining, as well as providing some theoretical and technical support for solving the problem of secure data mining in outsourced cloud computing environment.

6. Conclusions

This paper focused on reviewing existing research works of secure outsourced association rule mining in cloud computing environment. We summarized and analyzed three aspects of this research direction, i.e., privacy protection of outsourced association rule mining, result verification and access control of outsourced cloud data mining. We also proposed some future research suggestions, which might be useful to build secure and efficient schemes of outsourced association rule mining. For future work, we plan to extend our research on other secure outsourced data mining tasks under more practical scenarios.

Acknowledgements

This research was funded by National Natural Science Foundation of China with grant number 62102447. It was also funded by Henan Key Laboratory of Network Cryptography Technology with grant number LNCT2022-A16.

References

[1] Wong W K, Cheung D W, Hung E, et al. Security in outsourcing of association rule mining [C]. In Proceedings of the 33rd international conference on Very large databases. 2007: 111-122.
[2] Tai C-H, Yu P S, Chen M-S. k-Support anonymity based on pseudo taxonomy for outsourcing of frequent itemset mining [C]. In Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining. 2010: 473–482.
[3] Giannotti F, Lakshmanan L V, Monreale A, et al. Privacy-preserving mining of association rules from outsourced transaction databases [J]. IEEE Systems Journal. 2013,7 (3): 385–395.
[4] Li L, Lu R, Choo K-K R, et al. Privacy-preserving outsourced association rule mining on vertically partitioned databases [J]. IEEE Transactions on Information Forensics and Security. 2016, 11 (8): 1847–1861.
[5] Molloy I, Li N, Li T. On the (in) security and (im) practicality of outsourcing precise association rule mining [C]. In 2009 Ninth IEEE International Conference on Data Mining. 2009: 872–877.
[6] Wang B, Zhan Y, Zhang Z. Cryptanalysis of a symmetric fully homomorphic encryption scheme [J]. IEEE Transactions on Information Forensics and Security. 2018,13 (6): 1460–1467.

ISSN 2616-5775 Vol. 7, Issue 5: 207-214, DOI: 10.25236/AJCIS.2024.070527

[7] Lai J, Li Y, Deng R H, et al. Towards semantically secure outsourcing of association rule mining on categorical data [J]. Information Sciences. 2014, 267: 267–286.
[8] Lewko A, Okamoto T, Sahai A, et al. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption [C]. In Annual International Conference on the Theory and Applications of Cryptographic Techniques.2010: 62–91.
[9] Waters B. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions [C]. In Annual International Cryptology Conference. 2009:619–636.
[10] Yi X, Rao F-Y, Bertino E, et al. Privacy-preserving association rule mining in cloud computing [C]. In Proceedings of the 10th ACM symposium on information, computer and communications security. 2015: 439–450.
[11] Gennaro R, Jarecki S, Krawczyk H, et al. Secure distributed key generation for discrete-log based cryptosystems [J]. Journal of Cryptology. 2007, 20 (1): 51–83.
[12] Jakobsson M, Juels A. Mix and match: Secure function evaluation via ciphertexts[C]. In International Conference on the Theory and Application of Cryptology and Information Security. 2000: 162–177.
[13] Van Dijk M, Gentry C, Halevi S, et al. Fully homomorphic encryption over the integers [C]. In Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2010: 24–43.
[14] Liu J, Li J, Xu S, et al. Secure outsourced frequent pattern mining by fully homomorphic encryption [C]. In International Conference on Big Data Analytics and Knowledge Discovery. 2015: 70–81.
[15] Imabayashi H, Ishimaki Y, Umayabara A, et al. Secure frequent pattern mining by fully homomorphic encryption with ciphertext packing[M]//Data Privacy Management and Security Assurance. Springer, Cham, 2016: 181-195.
[16] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping [J]. ACM Transactions on Computation Theory (TOCT).2014, 6 (3): 13.
[17] Smart N P, Vercauteren F. Fully homomorphic SIMD operations [J]. Designs, codes and cryptography. 2014, 71 (1): 57–81.
[18] Qiu S, Wang B, Li M, et al. Toward practical privacy-preserving frequent itemset mining on encrypted cloud data [J]. IEEE Transactions on Cloud Computing. 2017.
[19] Paillier P, et al. Public-key cryptosystems based on composite degree residuosity classes [C]. In Eurocrypt. 1999: 223–238.
[20] Boneh D, Goh E-J, Nissim K. Evaluating 2-DNF formulas on ciphertexts [C].In Theory of Cryptography Conference. 2005: 325–341.
[21] Liu L, Su J, Chen R, et al. Privacy-Preserving Mining of Association Rule on Outsourced Cloud Data from Multiple Parties [C]. In Australasian Conference on Information Security and Privacy. 2018: 431–451.
[22] Bresson E, Catalano D, Pointcheval D. A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications [C]. In International Conference on the Theory and Application of Cryptology and Information Security. 2003:37–54.
[23] Wei Wu, Ming Xian, Udaya Parampalli, and Bin Lu. Efficient privacy-preserving frequent itemset query over semantically secure encrypted cloud database [J]. World Wide Web, 24(2):607–629, 2021.
[24] Bos, J.W., Lauter, K., Loftus, J., Naehrig, M.: Improved security for a ring-based fully homomorphic encryption scheme [C]. In: IMA International Conference on Cryptography and Coding. Springer, pp 45–64, 2013.
[25] Wong W K, Cheung D W, Hung E, et al. An audit environment for outsourcing of frequent itemset mining [C]. In Proceedings of the VLDB Endowment. 2009: 1162–1173.
[26] Dong B, Liu R, Wang H. Result Integrity Verification of Outsourced Frequent Itemset Mining [C]. In IFIP Annual Conference on Data and Applications Security and Privacy. 2013: 258–265.
[27] Liu R, Wang H. Result integrity verification of outsourced privacy-preserving frequent itemset mining[C]//Proceedings of the 2015 SIAM International Conference on Data Mining. Society for Industrial and Applied Mathematics, 2015: 244-252.
[28] Dong B, Liu R, Wang W H. Integrity Verification of Outsourced Frequent Itemset Mining with Deterministic Guarantee [C]. In IEEE International Conference on Data Mining. 2013: 1025–1030.
[29] Dong B, Liu R, Wang H W. Trust-but-verify: Verifying result correctness of outsourced frequent itemset mining in data-mining-as-a-service paradigm[J]. IEEE Transactions on Services Computing, 2015, 9(1): 18-32.
[30] Rong H, Wang H, Liu J, et al. Verifiable and privacy-preserving association rule mining in hybrid cloud environment[C]//Green, Pervasive, and Cloud Computing: 13th International Conference, GPC 2018, Hangzhou, China, May 11-13, 2018, Revised Selected Papers 13. Springer International

ISSN 2616-5775 Vol. 7, Issue 5: 207-214, DOI: 10.25236/AJCIS.2024.070527

Publishing, 2019: 33-48.
[31] Rong H, Liu J, Wu W, et al. Toward fault-tolerant and secure frequent itemset mining outsourcing in hybrid cloud environment[J]. Computers & Security, 2020, 98: 101969.
[32] Zhang J, Xie X, Zhang Z. How reliable is your outsourcing service for data mining? A metamorphic method for verifying the result integrity[C]//International Conference on Software Analysis, Testing, and Evolution. Cham: Springer International Publishing, 2018: 120-136.
[33] Hong T P, Chiu C C, Su J H, et al. Applicable Metamorphic Testing for Erasable-Itemset Mining[J]. IEEE Access, 2022, 10: 38545-38554.
[34] Zhao Z, Lan L, Wang B, et al. Verifiable Privacy-Preserving Outsourced Frequent Itemset Mining on Vertically Partitioned Databases[J]. Electronics, 2023, 12(8): 1952.
[35] Chen Y, Zhao Q, Duan P, et al. Verifiable privacy-preserving association rule mining using distributed decryption mechanism on the cloud[J]. Expert Systems with Applications, 2022, 201: 117086.
[36] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing[C]//International conference on the theory and application of cryptology and information security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001: 514-532.
[37] Döttling N, Garg S. Identity-based encryption from the Diffie-Hellman assumption[C]//Annual International Cryptology Conference. Springer, Cham, 2017: 537-569.
[38] Deng H, Qin Z, Wu Q, et al. Identity-based encryption transformation for flexible sharing of encrypted data in public cloud[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 3168-3180.
[39] Li J, Yu Q, Zhang Y. Hierarchical attribute based encryption with continuous leakage-resilience[J]. Information Sciences, 2019, 484: 113-134.
[40] Li J, Yu Q, Zhang Y, et al. Key-policy attribute-based encryption against continual auxiliary input leakage[J]. Information Sciences, 2019, 470: 175-188.
[41] Xue L, Yu Y, Li Y, et al. Efficient attribute-based encryption with attribute revocation for assured data deletion[J]. Information Sciences, 2019, 479: 640-650.
[42] Koppula V, Waters B. Realizing chosen ciphertext security generically in attribute-based encryption and predicate encryption[C]//Annual International Cryptology Conference. Springer, Cham, 2019: 671-700.
[43] Li J, Zhang Y, Ning J, et al. Attribute based encryption with privacy protection and accountability for CloudIoT[J]. IEEE Transactions on Cloud Computing, 2020.
[44] Xue L, Yu Y, Li Y, et al. Efficient attribute-based encryption with attribute revocation for assured data deletion[J]. Information Sciences, 2019, 479: 640-650.
[45] Lai J, Deng R H, Guan C, et al. Attribute-based encryption with verifiable outsourced decryption[J]. IEEE Transactions on information forensics and security, 2013, 8(8): 1343-1354.
[46] Feng C, Yu K, Aloqaily M, et al. Attribute-based encryption with parallel outsourced decryption for edge intelligent IoV[J]. IEEE Transactions on Vehicular Technology, 2020, 69(11): 13784-13795.
[47] Premkamal P K, Pasupuleti S K, Alphonse P J A. A new verifiable outsourced ciphertext-policy attribute based encryption for big data privacy and access control in cloud[J]. Journal of Ambient Intelligence and Humanized Computing, 2019, 10(7): 2693-2707.
[48] Zheng H, Shao J, Wei G. Attribute-based encryption with outsourced decryption in blockchain[J]. Peer-to-Peer Networking and Applications, 2020, 13: 1643-1655.