JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 2129 - 2134
https://publishoa.com
ISSN: 1309-3452

A Survey on Public-Key and Identity-Based Encryption Scheme with Equality Testing over Encrypted Data in Cloud Computing

Dr. M. Gobi[1], B. Arunapriya[2]

[1]Assistant Professor,
Department of Computer Science,
Chikkanna Government Arts College, Tiruppur, India.
Email: mgobimail@yahoo.com

[2]Research scholar,
Department of Computer Science,
Chikkanna Government Arts College, Tiruppur, India.
Email: arunapriyanataraj@gmail.com.

ABSTRACT

Cloud computing is a high demanding technology since the users and their data are increasing extremely day-by-day. Through an extensive utilization of cloud computing and storage devices, sensitive data is increasingly centralized into the cloud for reducing the maintenance cost which increases concerns about data privacy. One of the promising techniques to maintain the confidentiality of outsourced sensitive data is encryption schemes, however effective data utilization and also an efficient searching on encrypted data in cloud security are still challenging processes. Over the decades, many encryption techniques, namely Public-Key Encryption (PKE) and Identity-Based Encryption (IBE) with keyword searching and Equality Testing (ET) have been adopted to tackle those challenges over the encrypted data, but Private Matching (PM) over encrypted data is still difficult. In this paper, different researches based on PKEET and IBEET schemes in cloud computing are briefly studied which are utilized for data authorization and privacy-preserving. In addition, a comparative analysis is conducted to address the limitations in those schemes and suggest a further solution to tackle the identified issues. This survey helps us to overcome the PM over encrypted data in IBEET schemes and simplify the certificate management.

Keywords—Cloud computing, Public-key encryption, Identity-based encryption, Private matching, Keyword search, Equality test

I. INTRODUCTION

Cloud computing is a novel technology for a long vision of computing as a utility and has been achieving a huge deal of energy in the Information Technology (IT) industry. Several organizations, enterprises and even individuals outsource their data into the cloud and thus to have the on-demand high quality data storage services and computing resources. Although such benefits, data outsourcing denies the data owners of direct control over their own outsourced data which could expose few private sensitive data such as Personal Health Records (PHR), facebook images, economic transactions or industrial files. Nowadays, cloud health monitoring using PHR becomes the most popular technology in real world which reduces the burden of visiting the hospital for everything. It enables the users to retrieve the health care details at the time of emergency situation without the need of go to hospital directly. These processes can be done only by storing the personal health record details of the patients in the cloud environment. When the cloud users are storing their personal health records in the cloud environment which will lead to a security issue where there is a possibility of corruption or leakage of sensitive information to the cloud service providers who is not trustable one. So that, the cloud users started to store their personal information into the cloud environment in the encrypted format and limit the data access control [1].

To maintain the privacy of owner's sensitive data against suspicious cloud servers, data encryption before outsourcing is a promising solution. Different encryption schemes have been adopted to solve few data privacy problems is PHR systems and mobile social networks. On the other hand, data encryption may strictly obstruct a number of functionalities of data

eg., private matching over outsourced encrypted datasets. Privacy Matching (PM) has been applied widely in the cloud computing concept such as privacy-preserving data mining [2], mobile social networks or discovering family spirits in an internet-based PHR. Most of the techniques can perform searches on encrypted data such as Public-Key Encryption (PKE) with keyword search and Equality Testing (ET). These methods have certificate management issues and not suitable for large-scale datasets. Therefore, Identity-Based Encryption (IBE) has been introduced to tackle these issues by using identity for encryption [3].

The main aim of this article is to present a detailed survey on PKEET and IBEET schemes over encrypted data in cloud computing. Initially, different authorization schemes such as PKEET or IBEET over encrypted data in cloud computing. Also, a comparative analysis is carried out in terms of advantages and disadvantages to address the limitations in those schemes and suggest the further enhancement on IBEET scheme in cloud computing.

The rest of the article is structured as follows: Section II presents the detailed study on previous researches related to the PKEET and IBEET schemes in cloud computing. Section III illustrates the comparative analysis of those schemes and Section IV concludes the entire discussion.

II. LITERATURE SURVEY

Li et al. [4] investigated an essential of search capability authorization was studied using online Personal Health Record (PHR). Also, a scalable fine-grained authorization framework was established for Authorized Private Keyword Search (APKS) over encrypted data in the cloud computing. In this framework, the search capabilities of each user under the authorization of Local Trusted Authorities (LTA) were obtained based on checking for user's attributes. Then, two novel solutions were proposed for APKS based on the advanced cryptographic primitive, Hierarchical Predicate Encryption (HPE). Further, the query privacy was enhanced that hides user's query keywords against the server.

Tang [5] investigated a type of public key encryption schemes that supports plaintext equality test and user-specified authorization. A new primitive All-or-Nothing-Public Key Encryption supporting plaintext Equality Test (AoN-PKEET) was proposed that introduces an authorization mechanism for users for specifying who can perform plaintext equality test from their ciphertexts. In addition, a secure PHR application was constructed in which patients can encrypt their PHR and outsource the ciphertexts to a third-party service provider. Further, this cryptosystem was enhanced by integrating the concept of computational client puzzles for mitigating the risks against the semi-trusted proxies.

Li et al. [6] proposed a scalable and secure sharing of PHR in cloud computing using Attribute-Based Encryption (ABE). In this method, a novel patient-centric framework and a suite of mechanisms were proposed for data access control to PHR stored in semi-trusted servers. The ABE techniques were leveraged for encrypting each patient's PHR file and achieving fine-grained and scalable data access control for PHR. In this method, multiple data owner scenario was focused and the users in the PHR system were spilt into multiple security domains that greatly reduce the key management complexity for owners and users. A high degree of patient privacy was ensured simultaneously by exploiting multi-authority ABE.

Li et al. [7] proposed FindU i.e., a set of privacy-preserving distributed profile matching schemes for proximity-based mobile social networks. In this method, an initiating user may find from a group of users the one whose profile best matches with his/her for limiting the risk of privacy exposure only required and minimal information about the private attributes of the participating users was exchanged. Two increasing levels of user privacy were defined with decreasing amounts of revealed profile information. Tow fully distributed privacy-preserving profile matching schemes such as Private Set-Intersection (PSI) and Private Cardinality of Set-Intersection (PCSI) protocols were proposed by leveraging Secure Multi-party Computation (SMC) techniques that realize each of the user privacy levels which can also be personalized by the users.

Wang et al. [8] proposed a privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud computing. In this method, a novel multi-keyword fuzzy search scheme was proposed by exploiting the Locality-Sensitive Hashing (LSH) technique. The LSH functions in the Bloom filter were leveraged for constructing the file index and an efficient solution was provided to the secure fuzzy search of multiple keywords. As well, the Euclidean distance was adopted for capturing the similarity between the keywords and the secure inner product computation was used for computing the similarity score

which enables the result ranking. Further, a basic scheme including an improved scheme was proposed for achieving different security requirements.

Wu et al. [9] proposed a communication-efficient private matching scheme in client-server model. This scheme was proposed based on the Oblivious Transfer (OT) protocol for constructing the private matching for further improving the communication-efficiency. The major objective was reducing the size of the client and server's index universe. The size of the hashed index universe was determined based on the security parameter. A respective private matching applicable function was built based on the universal hash function borrowed from randomized algorithms. An approximate private-matching was defined by relaxing the definition of the original private matching for modeling the mismatch and information leakage.

Shao & Yang [10] proposed the PKE with keywords search into the problem of secure two-party computation and a novel approach was proposed for accomplishing PSI which utilizes PKE with keywords search as the fundamental tool. The major objective of this approach was achieving PSI in computationally asymmetric settings which can be instantiated by cloud computing. This approach does not require the expensive MapToPoint operation. Therefore, the computation complexity was reduced significantly.

Zheng & Xu [11] proposed the novel notion of Verifiable Delegated Set Intersection (VDSI) on outsourced encrypted data. The main objective was delegating e the set intersection operation to the cloud while not giving the decryption capability to the cloud and being able to hold the misbehaving cloud accountable. The security properties of VDSI were formalized and a concrete VDSI scheme was presented. This scheme was based on two concepts such as (i) using proxy re-encryption to enable the cloud to compare equality of plaintexts corresponding to two ciphertexts that are encrypted using different public keys (ii) using a novel variant of cryptographic accumulator which can be used to verify the membership of multiple elements through a single examination and may be of independent value to allow the cloud to show the correctness of the resulting intersection set.

Huang et al. [12] proposed semantic secure PKE with Filtered Equality Test (PKE-FET) based on the properties of secret sharing and bilinear map for improving the equality test over encrypted data in the cloud computing. In this scheme, an additional functionality was provided to conventional PKE. The sender uses the receiver's public key to produce encrypted data, and delivers them to the server. The receiver designates a set of messages to generate its warrant and delivers to the server. Once the server holds warrants and ciphertexts, it does the check without decryption when the hidden message belongs to that message set. In ABE schemes, those ones who match the settled conditions could get the privilege of decryption. In FET schemes, those messages inside selected set can be equality tested.

Ma [13] proposed an IBE with outsourced Equality Test (IBEET) in cloud computing. Initially, the concepts of PKEET and IBE were combined for obtaining IBEET. In this scheme, the receiver computes a trapdoor by using the secret value for the identity and then transmits it to a cloud server for equality test on its ciphertexts with other's ciphertexts. Also, a One-Way Chosen-Ciphertext security against a chosen Identity Attack (OW-ID-CCA) was defined and a concrete construction was proposed in the bilinear pairing. This cryptography primitive extends IBE with keyword search for yielding a common function i.e., equality test which maintains the function of keyword search trivially. Moreover, the equality test was performed on different user's ciphertexts including on single user's ciphertexts.

Huang et al. [14] proposed a secure data sharing and profile matching scheme for mobile healthcare social networks in cloud computing. In this scheme, the patients can outsource their encrypted health records to cloud storage with Identity-Based Broadcast Encryption (IBBE) technique and distribute them with a group of doctors in a secure and efficient manner. After that, an attribute-based conditional data re-encryption construction was presented that facilitates the doctors who satisfy the pre-defined conditions in the ciphertext for authorizing the cloud platform that converts the ciphertext into a new ciphertext of an IBE scheme for specialist without leaking any sensitive data. Moreover, a profile matching mechanism was proposed based on the IBE with equality test to support the patients for finding friends in a privacy-preserving manner and achieving a flexible authorization on the encrypted health records with resisting the keywords guessing attack.

Qiu et al. [15] proposed an Identity-Based Private Matching (IBPM) scheme to realize the fine-grained authorization that enables the privileged cloud server for performing private matching operations without leaking any private data. The

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 2129 - 2134
https://publishoa.com
ISSN: 1309-3452

rigorous security proof was presented under the Decisional Linear Assumption (DLN) and Decisional Bilinear Diffie-Hellman Assumption (DBDH). Further, this IBPM scheme was applied for solving the problems of fuzzy private matching and multi-keyword fuzzy search by constructing two efficient schemes such as identity-based fuzzy private matching and identity-based multi-keyword fuzzy search.

III. RESULTS AND DISCUSSIONS

In this section, a comparative analysis of IBE methods over encrypted data in cloud computing studied in the above section is presented in terms of their merits and demerits. The following Table 1 gives the merits and demerits of the above mentioned IBE-based private matching techniques over encrypted data in cloud computing.

Table.1 Comparison of Different Researches on PKEET/IBEET Schemes in Cloud Computing

Ref. No.	Techniques	Merits	Demerits	Performance Metrics
[4]	APKS based on advanced cryptographic primitive, HPE	Achieves a high level of system scalability.	High complexity.	Length of ciphertext and secret key, n=73: Projected total search time=2498sec
[5]	AoN-PKEET	Higher level of security guarantees.	The encrypted keywords and messages may not be consistent with each other that lead an inconsistent encryption.	Computational complexity: Encryption=4 Exp; Decryption=2 Exp; ET=2 Exp (Exp: Exponentiation)
[6]	Multi-authority ABE	High efficiency, scalability, flexibility and usability.	Data encryption may strictly obstruct PM over outsourced encrypted data.	-Nil-
[7]	PSI and PCSI	Better efficient and achieves security guarantees.	It does not absolutely prevent the user profiling.	PSI: Total computation time=0.14sec; Total sent bytes=2080KB PCSI: Total computation time=0.093sec; Total sent bytes=4326KB
[8]	Privacy-preserving multi-keyword fuzzy search	Better efficiency and suitability.	IB multi-keyword fuzzy search was not studied yet.	Number of keywords=10: Index generation time=200sec; Search time=128ms Number of documents=2500: Index encryption time=160sec; Search time=300ms
[9]	Communication-efficient private matching scheme based on OT protocol	Less computation and communication overhead.	It requires an efficient PM protocol against malicious adversaries.	-Nil-
[10]	PKE with keywords search	Less computation complexity.	It requires more efficient techniques to improve efficiency and security.	-Nil-
[11]	VDSI	Less computation and	Requires fine-grained access control to	Size of intersection set/size of dataset=75% (VDSI-User):

		communication cost.	improve higher level of security.	Computation time=1400sec; Communication overhead=10MB
[12]	PKE-FET	Better security.	Less efficiency due to massive bilinear mapping operations.	-Nil-
[13]	IBEET, OW-ID-CCA	Higher security.	High computational complexity.	-Nil-
[14]	IBBE technique	Better data security and privacy.	High computation time.	Computation time: TrapGen-1=0.0166ms; TrapGen-2=5.4253ms; Test-1=62.0125ms; Test-2=57.1098ms; Test-3=51.4711ms
[15]	IBPM, DLN, DBDH	More efficient.	When the dataset become large, the communication cost may take large bandwidth usage.	Average execution time for different algorithms (Size of dataset=2^{15}): KeyGen=0.058sec; Enc=3679.9sec; Dec=364.2sec; Aut=0.089sec; Mat=2984.5sec

IV. CONCLUSION

In this article, a detailed comparative study on encryption techniques such as PKEET and IBEET in cloud computing. Through this comparative analysis, it is obvious that all researchers have practiced on PKEET and IBEET for achieving fine-grained authorization on the encrypted data in cloud computing. Among those different schemes, IBPM scheme was computationally efficient and practical. Even though, still this scheme has few limitations, e.g., the communication cost may get larger bandwidth usage while the dataset becomes large enough. Therefore, the future extension of this study could further reduce communication and computational complexity of IBPM over outsourced encrypted data in cloud computing with increased security.

REFERENCES

[1] Lu, Y., & Tsudik, G. (2011, June). Enhancing data privacy in the cloud. In *IFIP International Conference on Trust Management* (pp. 117-132). Springer, Berlin, Heidelberg.

[2] Aggarwal, C. C., & Philip, S. Y. (2008). A general survey of privacy-preserving data mining models and algorithms. In *Privacy-preserving data mining* (pp. 11-52). Springer, Boston, MA.

[3] Chen, R., Mu, Y., Yang, G., Guo, F., & Wang, X. (2015, June). A new general framework for secure public key encryption with keyword search. In *Australasian Conference on Information Security and Privacy* (pp. 59-76). Springer, Cham.

[4] Li, M., Yu, S., Cao, N., & Lou, W. (2011). Authorized private keyword search over encrypted data in cloud computing. In *2011 31st International Conference on Distributed Computing Systems* (pp. 383-392). IEEE.

[5] Tang, Q. (2012). Public key encryption supporting plaintext equality test and user-specified authorization. *Security and Communication Networks*, *5*(12), 1351-1362.

[6] Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE transactions on parallel and distributed systems*, *24*(1), 131-143.

[7] Li, M., Yu, S., Cao, N., & Lou, W. (2013). Privacy-preserving distributed profile matching in proximity-based mobile social networks. *IEEE Transactions on Wireless Communications*, *12*(5), 2024-2033.

[8] Wang, B., Yu, S., Lou, W., & Hou, Y. T. (2014). Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud. In *IEEE INFOCOM 2014-IEEE Conference on Computer Communications* (pp. 2112-2120). IEEE.

[9] Wu, M. E., Chang, S. Y., Lu, C. J., & Sun, H. M. (2014). A communication-efficient private matching scheme in Client–Server model. *Information Sciences*, *275*, 348-359.

[10] Shao, Z. Y., & Yang, B. (2015). Private set intersection via public key encryption with keywords search. *Security and Communication Networks*, *8*(3), 396-402.

[11] Zheng, Q., & Xu, S. (2015). Verifiable delegated set intersection operations on outsourced encrypted data. In *2015 IEEE International Conference on Cloud Engineering* (pp. 175-184). IEEE.

[12] Huang, K., Chen, Y. C., & Tso, R. (2015). Semantic secure public key encryption with filtered equality test PKE-FET. In *2015 12th International Joint Conference on e-Business and Telecommunications (ICETE)* (Vol. 4, pp. 327-334). IEEE.

[13] Ma, S. (2016). Identity-based encryption with outsourced equality test in cloud computing. *Information Sciences*, *328*, 389-402.

[14] Huang, Q., Yue, W., He, Y., & Yang, Y. (2018). Secure identity-based data sharing and profile matching for mobile healthcare social networks in cloud computing. *IEEE Access*, *6*, 36584-36594.

[15] Qiu, S., Liu, J., Shi, Y., Li, M., & Wang, W. (2018). Identity-based private matching over outsourced encrypted datasets. *IEEE Transactions on Cloud Computing*, *6*(3), 747-759.