ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/323123557

Searchable Encryption: A Review

Article *in* International Journal of Security and its Applications · December 2017

DOI: 10.14257/ijsia.2017.11.12.07

CITATIONS
4

READS
2,512

4 authors:

Khadijah Chamili
USIM | Universiti Sains Islam Malaysia
4 PUBLICATIONS **21** CITATIONS
SEE PROFILE

Md Jan Nordin
Universiti Kebangsaan Malaysia
125 PUBLICATIONS **806** CITATIONS
SEE PROFILE

Waidah Ismail
USIM | Universiti Sains Islam Malaysia
42 PUBLICATIONS **148** CITATIONS
SEE PROFILE

Abduljalil Radman
Taiz University
24 PUBLICATIONS **189** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Heterogeneous Face Recognition in Video Surveillance System View project

Reconstruction of Ancient Two-Dimensional Objects View project

All content following this page was uploaded by Waidah Ismail on 05 April 2018.

The user has requested enhancement of the downloaded file.

Searchable Encryption : A Review

Khadijah Chamili[1,2], Md. Jan Nordin[2]
[1]Universiti Sains Islam Malaysia,
[2]Faculty of Information Science & Technology,
Universiti Kebangsaan Malaysia,
khadijah@usim.edu.my, jan@ukm.edu.my

Waidah Ismail, Abduljalil Radman
Faculty of Science & Technology,
Universiti Sains Islam Malaysia[3],
waidah@usim.edu,my, abdu_rad@yahoo.com

***Abstract*— Cloud computing is one of the most important technologies which supports reliability, scalability, ease of deployment and cost efficient to business growth. Despite its benefits, cloud computing still has open and remain challenges on ensuring confidentiality, integrity, and availability (CIA) of sensitive data located on it. As a solution, the data is encrypted before sending to the cloud. However, the normal searching analogy couldn't get through the encrypted data. In this paper, Searchable Encryption (SE) techniques which allow accessing data on encrypted cloud were reviewed and classified. Nine SE techniques were presented with different issues and characteristics on achieving secrecy and efficiency of SE. Four main characteristics of SE were also identified and categorized for future works on SE.**

Keywords—Searchable Encryption, Cloud, Encryption, Review, Survey

I. INTRODUCTION

Electronic Health Record (EHR) systems have widely adopted to keep patient information and their medical records in a proper manner [1]. EHR systems benefit in costs and time reduction, quality of care improvement and data sharing among stakeholders [1], [2]. Cloud computing is one of advent technologies that support easy deployment application like EHR systems with a low-cost implementation which offer Pay-Per-Use basis [3], [4], [5], [6], [7]. The emergence of cloud or mobile computing dramatically emerges the growth of the mobile commerce, mobile learning, mobile health and mobile gaming [8] which acquire availability and reliability of services 24 by 7. These make cloud computing services on demand and in trend due to its scalability, dynamic provisioning, ease of integration and support multi-tenant [8].

Despite cloud computing beneficial, there's still remaining issues and challenges on ensuring confidentiality, integrity, and availability (CIA) of protection and security of personal information which is critical in the health sector [1]. Personal information (e.g. identity number, telephone number, address) is usually stored in cloud computing which always considered as a untrusted or semi-trusted server [3], [5]. This untrusted server tends to contribute to the privacy and security issues [3], [4], [5], [6]. One of the main security issues is data confidentiality. Data confidentiality is to ensure sensitive data (e.g. personal information) is safe from unauthorized access. Recently, cryptography or encryption is regarded as a promising method for data confidentiality [5], [7], [8].

Cryptography or encryption is about to secure a communication over an insure channel [9]. However, traditional search mechanisms do not work for encrypted data [10], [11]. One of the solutions is using Searchable Encryption (SE) which enable users to secure search on encrypted data stored in the cloud [4]. In this paper, the searchable encryption methods developed in the literature are reviewed and classified based on technique utilized.

The rest of this paper is organized as follows. We first review issues motivate to SE works and nine SE techniques with related works in Section II. In Section 3, we discuss factors which affect SE performance. 4. Lastly, we conclude this paper with suggestion on combination SE technique while applying SE in future works.

II. SEARCHABLE ENCRYPTION (SE)

SE is a term of searching on encrypted data located on untrusted server or cloud without the need to decrypt [11]. In 2000 Song et al. proposed the idea of SE scheme which solves the issue on searching encrypted data on cloud. According to C. Bosch et al. [12], SE scheme has six SE techniques (Fig. 1), and still rapidly growth until now. These six SE techniques include Searchable Symmetric Encryption (SSE), Public Key with Keyword Search (PEKS), Identity-Based Encryption (IBE), Hidden Vector Encryption (HVE), Predicate

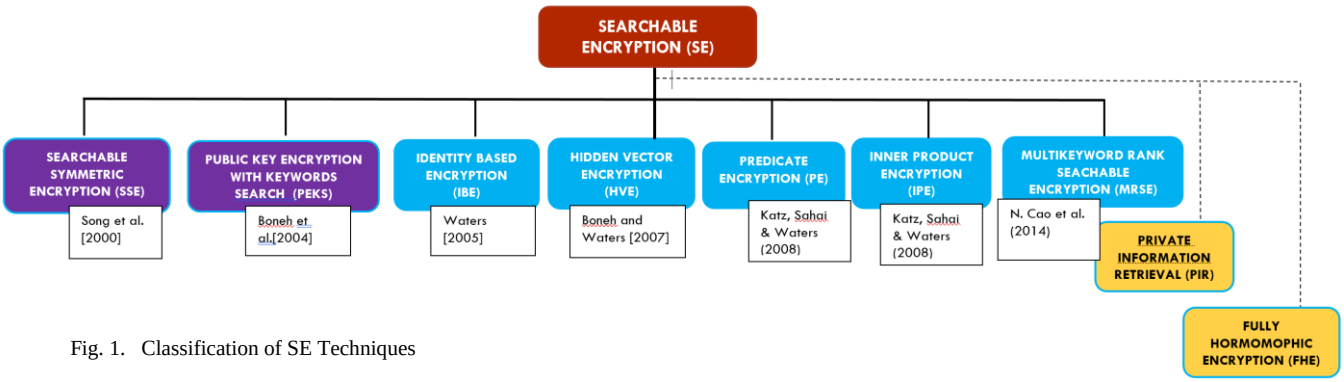

Fig. 1. Classification of SE Techniques

Encryption (PE), and Inner Product Encryption (IPE). Moreover, recent study [3] has regarded that Multi-keyword Rank Searchable Encryption (MRSE) is as a new SE technique. Based on the literature review has been done for last seven years as shown in Fig. 2, we can see the intention from academia and industry in SE are tremendously increased from year to year.

However, the techniques are shown in Fig. 1 remain unchallenged issues. They are developed to maintain secure and efficient communication between client and server on cloud [11]. They also support single user architecture [11] and multi-user architecture [10]. In addition, works done to support single keyword search [11], [13], multi-keyword search and ranking [3], [14], [15], subset query and range query [16], [17] and fuzzy multi-keyword search [18], [19]. Most of the previous works done on SE to improve secrecy motivated by adversary activity [20], [21]. Some adversary activities include brute force attack [20], search / access pattern leakage [8], [21] and DDoS attack [5]. To proof that any scheme or algorithm developed was resistant enough from attacks or adversary activities, system model and threat model were constructed for experimental purposes [3], [14]. In other works, other techniques like Private Information Retrieval (PIR) [22] and Fully Homomorphic Encryption (FHE) [23] were considered in enhancing SE.

A. Symmetric Searchable Encryption

Symmetric Searchable Encryption (SSE) allows the user to upload data to the cloud with provable secrecy by issuing isolated and hidden query [11]. Hidden query and isolation query allow the server to learn nothing about the plaintext except the ciphertext. The query is running as an encrypted query which called as trapdoors: trapdoors are always generated using secret key [11]. The SSE probabilistic algorithm as below:

- Keygen(1^k): a key generation algorithm run by the data owner. It takes a security parameter k as input, and outputs a secret key K.
- BuildIndex(K, D): a keyword index generation algorithm run by the data owner. It takes a secret key K and a set of documents D as inputs, and outputs a keyword index I.
- Trapdoor(K, w): a keyword trapdoor generation algorithm run by the user. It takes a secret key K and a query keyword w as inputs, and outputs the trapdoor Tw for the keyword w.
- Search(I, Tw): a keyword search algorithm run by the server. It takes a keyword index I and a trapdoor Tw as inputs, and outputs a set of documents D(w) that contains query keyword w.

Indeed, SSE is considered more suitable for outsourcing data of company or organization application system on the cloud or untrusted server [4], [11]. It supports client / server architecture. For example, Alice encrypts data with her secret key which generate by KeyGen algorithm. To encrypt data, two algorithms run: Enc algorithm and BuildIndex algorithm [4]. These algorithms generate ciphertext (encrypted data) together with an encrypted index. Then, both encrypted data and index are sent to the cloud. To search the encrypted data, for example, Bob runs a query or trapdoor by issuing Trapdoor algorithm. Trapdoor algorithm encrypts the query request to the server on behalf of Bob. Next, the search algorithm computes the Trapdoor with encrypted index before the result is returned. The framework in Figure 3 illustrates SE.

SSE was practical solution attaining search time that was linear to the data size. However, it was not secure against statistical analysis (e.g. access pattern), one would run the same trapdoors for few times would expose to an adversary through statistic approaches.

To overcome the security issue, Goh [24] proposed constructions that associate an “index” to each document in a collection. This was called semantic security against adaptively chosen keyword attack (IND-CKA) and a slightly stronger IND2-CKA. He also developed an IND-CKA secure index called Z-IDX which utilizes Bloom filter to build an index for each data file. On the other hand, Curtmola et al. [25], revisited the SSE definition by using Oblivious RAM for stronger security definition which does not leak any information to the attacker/adversary.

In recent works, S. Dai et al. [26] constructed two memory leakage-resilient searchable symmetric encryption (MLR-SSE) scheme based on SSE and physic unclonable functions (PUFs) [27]. The PUFs is an equal function like hash function where it applies one-way function. The one-way function was introduced by O. Goldreich et al. [28] where it has below criteria :

- Easy to compute: There exists a deterministic P-time algorithm A such that on input x, A outputs f(x) (that is, A(x) = fix))
- Hard to invert: For every probabilistic P-time algorithm A', every positive polynomial p, and all sufficiently large n Pr(A'(f(U)).

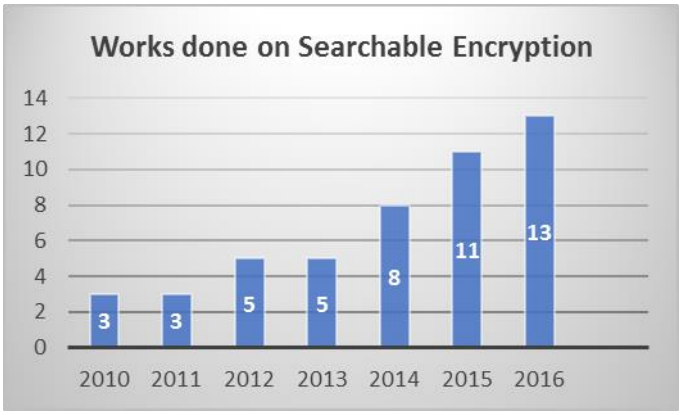

Fig. 2. Research works on Searchable Encryption within 7 years

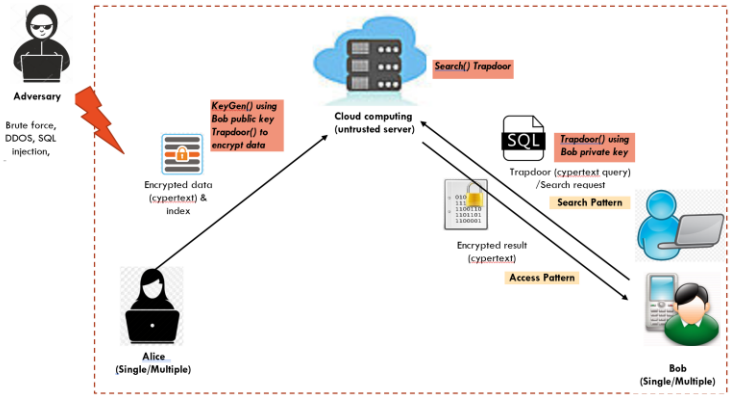

Fig. 3. Framework of Searchable Encryption

The combination of these two schemes enables high protection for the user's private key and efficiency. Efficiency only achieves with generating the secret key in real time by PUFs.

Furthermore, SSE has been applied to support secure channel between multiple located data [8]. C. Liu et al. [8] developed Multi-Data-Source DSSE (MDS-DSSE) to support dynamic social data such as chatting application system which proven secured against adaptive chosen-keyword attacks (CKA2). MDS-DSSE work was based on Dynamic Searchable Symmetric Encryption (DSSE) [29], which is developed to support searching on encrypted data for very large datasets without leakage any information to the unauthorized use.

B. Public Key with Keyword Search

Public Key with Keyword Search (PEKS) was introduced by Boneh et al [13] in 2004. Boneh et al. was using receiver's public-key for encrypted message with keyword and only receiver would allow to decrypt using he/she private key. PEKS consist of 5 probabilistic polynomial-time algorithms as below:

- KeyGen(λ)→ (pkSE, skSE) : Given a security parameter λ, the public/ private key pair (pkSE, skSE) is generated.
- Enc(pkSE,m)→c : Given the public key pkSE and a message m, it generates a ciphertext c.
- PEKS(pkSE,w)→Sw : Given the public key pkSE and a keyword w, it generates a PEKS ciphertext Sw of w.
- Trapdoor(skSE,w)→Tw : Given a keyword w and the private key skSE, it produces a trapdoor Tw.
- Test(pkSE,Sw,Tw')→{0, 1} : Given the public key pkSE, a searchable encryption ciphertext Sw, and a trapdoor Tw', it outputs 1 (true) if w = w' or 0 (false) otherwise .

PEKS is mainly developed for data sharing scenario [4], [12], [13], for example putting mail on Email Service Provider like Gmail or Yahoo. With PEKS, Alice encrypts the data with Bob's public key by issuing KeyGen algorithm. Trapdoor algorithm is used to encrypt the data sent to the server. Once data requested by Bob through Trapdoor algorithm (query is in an encrypted manner) using Bob's private key, Test algorithm will compare keyword search and return to Bob if success.

Z. Deng et al. [10] used asymmetric searchable encryption to design multi-user searchable encryption scheme with keyword authorization (MSESKA). To construct multi-user setting, 6 polynomial-time algorithms were used. H.Yin et al. [17] developed a query privacy-enhanced secure search scheme based on secure index technique- Decisional Diffie–Hellman (DDH) and Bilinear Diffie–Hellman (BDH) assumptions together with bloom filter technique. This efficient secure search scheme with strong query privacy protection allow data user using randomly chosen secret keys every time query trapdoors were generated to the server.

In a different work, Secure Hybrid Indexed Search (SHIS) scheme was developed by W. Wang et al. [30] where semantic secure SHIS is a universal transformation from PEKS and DE to SHIS. The main idea behind the SHIS is to reduce the search complexity on PEKS by applying Dynamic Index (DI) and Static Index (SI). SI is applied to reduce the complexity of search from O(n) to O(u·w) (when first time search), and apply DI to reduce the complexity from O(n) to O(w) for the next query submission.

C. Identity Based Encryption

Identity Based Encryption (IBE) algorithm was initiated in 1984 by Shamir [31]. This scheme uses user's identity as a key for encryption and decryption process. User's identity key can be publicly accessed, which means that anyone can use it for sending a message. On the other hand, only the recipient with the private key can decrypt the message. For example, imagine the analogy of sending and receiving email, where recipient's email address which based on the recipient's name is used to send an email from the sender, while the recipient can open the email by using his/her email address.

PEKS is one of the main SE techniques that developed based on IBE [13]. IBE system which constructed by Bilinear Diffie-Hellman (BDH) proved that PEKS is semantically secure against a chosen keyword attack in the random oracle model. X. Dong et al. proposed a secure, efficient and scalable data collaboration scheme (SECO), in order to overcome one-to-many encryption paradigm, writing operation, and fine-grained access control issues in cloud communication through adopting two-level hierarchical identity-based encryption (HIBE) [32]. With SECO, data was encrypted with multiple recipient's public keys and only those users have the secret key would be allowed to access the data has been assigned to them. In this scheme, BDH was constructed in order to ensure SECO provides semantically secure and probabilistic.

D. Hidden Vector Encryption

Hidden Vector Encryption (HVE) is a type of predicate encryption (PE) that supports the fine-grained conjunctive combination of equality queries, comparison queries, and subset queries on encrypted data [33]. HVE is a specialized type of predicate encryption where two vectors over attributes are associated with a ciphertext and a token, respectively. At a higher level, the ciphertext matches the token if and only if the two vectors are component-wise equal. However, this simple equality predicate can be extended to support conjunctive combinations of equality, comparison, and subset predicates. The conjunction permits fine-grained search queries over encrypted data [34].

E. Predicate Encryption

Predicate encryption (PE) allows users search on encrypted data without a private key that corresponds to a public key. In a PE scheme, the token is provided for a query server regardless of the full private key. The query server then performs a test to identify matches ciphertext with the token supplied on particular predicates. If the test succeeds, the query server appropriately forwards the encrypted data to the private key owner without revealing any information to the server [35].

V. Goyal et al. [36] introduced Attribute-Based Encryption (ABE) which allows the sender to define who should be able to

read the data by setting up policy. In this scheme, private keys were distributed by an authority, that associated with sets of attributes and ciphertexts which also associated with formulas over attributes. A user with the distributed private key would able to decrypt the ciphertext as well as able to read the plaintext.

X.A. Wang et al. [37] claimed that PE could achieve more sophisticated and flexible functionality compared with traditional public key encryption. According to J. Katz [35] IBE, Anonymous IBE (AIBE) and attribute-based encryption schemes support range queries which considered under PE's framework.

F. Inner Product Encryption (IPE)

Inner Product Encryption (IPE) was first introduced by J. Katz et al. [35] which known as cryptographic mechanism that allows more fine-grained [33] (facilitate user with access to the data which fulfill the needs and requirement of the task given) with control over access to encrypt data. IPE cryptographic or known as *inner product computation* are most used in PE,IBE and HVE [38]. J. Katz et al. also managed to construct *attribute-hiding* schemes which handles disjunctions on polynomial-time predicates that is different from *payload-hiding* [33]. *Payload-hiding* is security notion to achieve stronger security level guarantees, where the ciphertext associated with attribute that hides all information until the secret key is possessed to decrypt. *Payload* and *attribute-hiding* slightly different in a way of ciphertext conceal of the plaintext. For *attribute-hiding*, the ciphertext should conceal together with associated parameter while *payload-hiding* only requires that a ciphertext conceal the plaintext [39].

G. Multi-keyword Ranked Search Encryption

Multi-keyword ranked search over encrypted cloud data (MRSE) was introduced in 2014 by N. Cao et al. [14]. The main idea of this scheme was to allow users on search request and return documents with semantic multiple keywords through "inner product similarity" keywords. In order to secure and get the most relevant results retrieval, MRSE was adapted from secure k-nearest neighbor (kNN) technique to select the k nearest database records between database record (p_i) and query vector (q). Secure inner product computation was adopted in order to set strict privacy requirement to ensure secrecy of cloud communication [14].

However, MRSE has three major drawbacks defined by R. Li et al [3]. First, MRSE is using a static dictionary which needs the dictionary to rebuild for every additional keyword, result presented in out-of-order form which difficult for user to get the most relevant file and lastly, MRSE does not consider the effects of keyword weight and access frequencies where keyword's file is not in the top list of the result. Therefore, R. Li proposed new flexible multi-keyword query scheme called MKQE to overcome MRSE's drawbacks. MKQE have successfully reduced the overhead maintenance during the keyword dictionary expansion by implementing the partitioned matrices approach. Furthermore, MQKE uses the weights of the keywords in the index file to solve the out-of-order problem in the matching result set.

H. Private Information Retrieval

Private Information Retrieval (PIR) protocol allows multiple readers to retrieve *i*th of *n*th bit data from multiple databases without revealing any information including access/search pattern to the server. PIR works significantly in smaller communication complexity than the obvious n-bit solution (meaning that it works with total communication less than the data size). It was first introduced in 1995 by E. Kushilevitz et al. [40]. However, PIR only allows keyword search on non-encrypted data [25].

I. Fully Hormomophic Encryption

FHE scheme is another technique to shorten the ciphertext and reduce the complexity of decryption through re-linearization (i.e. a process in reducing the size of the ciphertext back down to n+1) [41]. According to Gentry, FHE scheme security is strong enough and semantically secure [42]. Z. Brakerski [41] has applied FHE in SE by converting the symmetric ciphertexts into homomorphic ciphertexts without additional communication. X. Yi et al. [43] had developed single-database with PIR protocol using FHE which allows data to be encrypted only bit by bit in block database. This contributes to communication complexity $O(\underline{\nu}\log m+\underline{\nu}n/m)$ higher than $O(\log^2 n)$. Using PIR, communication is strictly smaller than n.

In the other hand, L. Tajan et al.[22] combined PIR protocol with Somewhat Homomorphic Encryption (SHE), and used SE on hiding which data of the evidence store is affected by the computation.

III. DISCUSSION

Based on our review, we found that SSE and PEKS are the most popular SE techniques used among the rest SE techniques described in Section 2. In general, SE technique is not limited for searching data but can be extended to add, delete and edit the data on the cloud. SE technique should be applied accordingly to the needs of the application system: efficiency, secrecy, architecture (e.g. single user, multiple user) and data type to be searched (keyword search). The needs of SE technique are illustrated in Fig. 4.

We understand that SE techniques were developed to meet particular needs as below:

- PEKS and HVE are for ensuring secure communication between two individuals (e.g. email sending from Alice to Bob)
- SSE is for online storage where single data are shared with multiple recipients.
- SSE and PEKS also are the best candidates to support the application with multi-user setting.
- Index tree based structure and FHE are more efficient compared to a vector which still needs an exhaustive search or expressive computation. Physical device such as Solid state disk (SSD) and PUF are to help on boosting the efficiency of SE.

- Fine-grained access control (IBE, HVE, PE, IPE) are applied to support role-based function.

However, for best implementation on ensuring privacy and efficiency, few techniques should be combined. This helps in constructing semantic security and boost efficiency on searching.

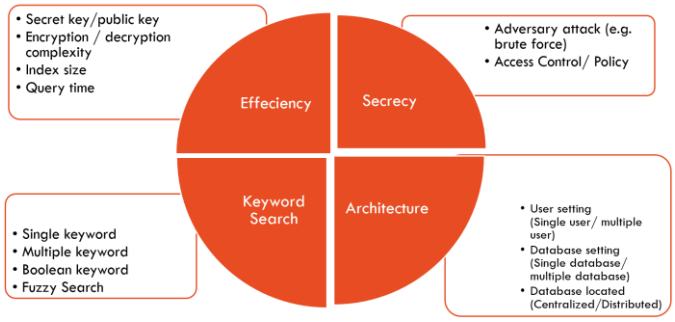

Fig. 4. Factors of Searchable Encryption

IV. CONCLUSION

We present nine SE techniques: SSE, PEKS, IBE, PE, IPE, HVE, MRSE, PIR and FHE as SE's family. SE techniques allow the user searching on encrypted cloud. The main goal of these SE techniques is to build secure and efficient communication between user and cloud. However, each one of these SE techniques have unique intention to achieve beside the main goal. Four main characteristics were identified which affect the SE performance on the cloud: efficiency, secrecy, keyword search and architecture. In conclusion, to develop strong and semantically secure with efficient communication, the combination of SE techniques should be considered in future works especially on EHR system.

ACKNOWLEDGMENT

This project is funded by Newton-Ungku Omar Fund: GRANT USIM/INT-NEWTON/FST/IHRAM/053000/41616.

REFERENCES

[1] J. L. Fernández-Alemán, I. C. Señor, P. ángel O. Lozoya, and A. Toval, 'Security and privacy in electronic health records: A systematic literature review', *J. Biomed. Inform.*, vol. 46, no. 3, pp. 541–562, 2013.

[2] Y. Yang, X. Zheng, and C. Tang, 'Lightweight distributed secure data management system for health internet of things', *J. Netw. Comput. Appl.*, 2016.

[3] R. Li, Z. Xu, W. Kang, K. C. Yow, and C. Z. Xu, 'Efficient multi-keyword ranked query over encrypted data in cloud computing', *Futur. Gener. Comput. Syst.*, vol. 30, no. 1, pp. 179–190, 2014.

[4] F. Han, J. Qin, and J. Hu, 'Secure searches in the cloud: A survey', *Futur. Gener. Comput. Syst.*, 2015.

[5] K.-K. R. Choo, J. Domingo-Ferrer, and L. Zhang, 'Cloud Cryptography: Theory, Practice and Future Research Directions', *Futur. Gener. Comput. Syst.*, vol. 62, pp. 51–53, 2016.

[6] Q. Liu, A. Srinivasan, J. Hu, and G. Wang, 'Preface: Security and privacy in big data clouds', *Futur. Gener. Comput. Syst.*, vol. 72, pp. 206–207, 2017.

[7] S. K. Pasupuleti, S. Ramalingam, and R. Buyya, 'An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing', *J. Netw. Comput. Appl.*, vol. 64, pp. 12–22, 2016.

[8] C. Liu, L. Zhu, and J. Chen, 'Efficient searchable symmetric encryption for storing multiple source data on cloud', *Proc. - 14th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2015*, vol. 1, pp. 451–458, 2015.

[9] S. Goldwasser, 'Lecture Notes on Cryptography', no. July, pp. 1–289, 2008.

[10] Z. Deng, K. Li, K. Li, and J. Zhou, 'A multi-user searchable encryption scheme with keyword authorization in a cloud storage', *Futur. Gener. Comput. Syst.*, p. , 2016.

[11] D. Wagner, A. Perrig, D. X. Song, D. Wagner, and A. Perrig, 'Practical techniques for searches on encrypted data', *Proceeding 2000 IEEE Symp. Secur. Priv.*, pp. 44–55, 2000.

[12] C. Bösch, P. Hartel, W. Jonker, and A. Peter, 'A Survey of Provably Secure Searchable Encryption', *ACM Comput. Surv.*, vol. 47, no. 2, pp. 1–51, 2014.

[13] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, 'Public Key Encryption with Keyword Search', *Proc. 23rd Annu. Int. Conf. Theory Appl. Cryptogr. Tech.*, pp. 506–522, 2004.

[14] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, 'Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data', no. 1, 2014.

[15] Y. Liu, Z. Li, W. Guo, and W. Chaoxia, 'Privacy-preserving multi-keyword ranked search over encrypted big data', *Third Int. Conf. Cybersp. Technol. (CCT 2015)*, no. 1, pp. 1–3, 2015.

[16] B. Zhang and F. Zhang, 'An efficient public key encryption with conjunctive-subset keywords search', *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 262–267, 2011.

[17] H. Yin, Z. Qin, L. Ou, and K. Li, 'A query privacy-enhanced and secure search scheme over encrypted data in cloud computing', *J. Comput. Syst. Sci.*, vol. 11, no. 16, pp. 311–14, 2016.

[18] M. Chuah and W. Hu, 'Privacy-aware bedtree based solution for fuzzy multi-keyword search over encrypted data', *Proc. - Int. Conf. Distrib. Comput. Syst.*, pp. 273–281, 2011.

[19] Z. Fu, X. Wu, C. Guan, and X. Sun, 'Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement', *IEEE Trans.*, no. July, 2016.

[20] L. Fang, W. Susilo, C. Ge, and J. Wang, 'Public key encryption with keyword search secure against keyword guessing attacks without random oracle', *Inf. Sci. (Ny).*, vol. 238, pp. 221–241, 2013.

[21] M. S. Islam, M. Kuzu, and M. Kantarcioglu, 'Access Pattern disclosure on Searchable Encryption: Ramification, Attack and Mitigation', *Ndss'12*, 2012.

[22] L. Tajan and C. A. Reuter, 'Private Information Retrieval and

Searchable Encryption for Privacy-Preserving Multi-Client Cloud Auditing', pp. 162–169, 2016.

[23] A. a Atayero and O. Feyisetan, 'Security Issues in Cloud Computing : The Potentials of Homomorphic Encryption', *J. Emerg. Trends Comput. Inf. Sci.*, vol. 2, no. 10, pp. 546–552, 2011.

[24] E.-J. Goh, 'Secure Indexes', *An early version this Pap. first Appear. Cryptol. ePrint Arch. Oct. 7th*, pp. 1–18, 2003.

[25] 平野貴人 *et al.*, 'Searchable Symmetric Encryption のドキュメント追加後の安全性について', *Scis 2012*, pp. 1–8, 2012.

[26] S. Dai, H. Li, and F. Zhang, 'Memory leakage-resilient searchable symmetric encryption', *Futur. Gener. Comput. Syst.*, vol. 62, pp. 76–84, 2016.

[27] P. S. Ravikanth, 'Physical One-Way Functions', *Science (80-.).*, 2002.

[28] O. Goldreich, L. a. Levin, and L. a Levint, 'A hard-core predicate for all one-way functions', *Proc. twenty-first Annu. ACM Symp. Theory Comput. - STOC '89*, pp. 25–32, 1989.

[29] D. Cash *et al.*, 'Dynamic Searchable Encryption in Very-Large Databases: Data Structures and Implementation', *Proc. 2014 Netw. Distrib. Syst. Secur. Symp.*, no. February, pp. 23–26, 2014.

[30] W. Wang, P. Xu, H. Li, and L. T. Yang, 'Secure hybrid-indexed search for high efficiency over keyword searchable ciphertexts', *Futur. Gener. Comput. Syst.*, vol. 55, pp. 353–361, 2016.

[31] '1998 (Shamir) - ID-basedCryptoSystem.pdf'. .

[32] X. Dong, J. Yu, Y. Zhu, Y. Chen, Y. Luo, and M. Li, 'SECO: Secure and scalable data collaboration services in cloud computing', *Comput. Secur.*, vol. 50, pp. 91–105, 2015.

[33] J. Katz, A. Sahai, and B. Waters, 'Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products', pp. 146–162.

[34] J. H. Park, 'Efficient hidden vector encryption for conjunctive queries on encrypted data', *IEEE Trans. Knowl. Data Eng.*, vol. 23, no. 10, pp. 1483–1497, 2011.

[35] J. Katz, A. Sahai, and B. Waters, 'Predicate encryption supporting disjunctions, polynomial equations, and inner products', *J. Cryptol.*, vol. 26, no. 2, pp. 191–224, 2013.

[36] V. Goyal, O. Pandey, A. Sahai, and B. Waters, 'Attribute-based encryption for fine-grained access control of encrypted data', *Proc. 13th ACM Conf. Comput. Commun. Secur. - CCS '06*, p. 89, 2006.

[37] X. A. Wang, F. Xhafa, W. Cai, J. Ma, and F. Wei, 'Efficient privacy preserving predicate encryption with fine-grained searchable capability for Cloud storage', *Comput. Electr. Eng.*, vol. 0, pp. 1–13, 2015.

[38] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, 'Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption', vol. 2, no. subaward 641, pp. 62–91.

[39] T. Okamoto and K. Takashima, 'Adaptively attribute-hiding (hierarchical) inner product encryption', *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. E99A, no. 1, pp. 92–117, 2016.

[40] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, 'Private information retrieval', *J. ACM*, vol. 45, no. 6, pp. 965–982, 1998.

[41] Z. Brakerski, 'Efficient Fully Homomorphic Encryption from (Standard) LWE', pp. 97–106, 2011.

[42] C. Gentry, 'Computing arbitrary functions of encrypted data', *Commun. ACM*, vol. 53, no. 3, p. 97, 2010.

[43] X. Yi, M. G. Kaosar, R. Paulet, and E. Bertino, 'Single-database private information retrieval from fully homomorphic encryption', *IEEE Trans. Knowl. Data Eng.*, vol. 25, no. 5, pp. 1125–1134, 2013.

.

View publication stats