



EFFICIENT DATA SHARING AND SEARCHING FOR SECURE CLOUD STORAGE

S.Chitra^{#1}, K.Nathiya^{#1}, I.Sadhiya^{#1}, A.Jainabee^{#1}, Mr.S.Hariprasath^{#2}

^{#1}Bachelor of computer science and Engineering

^{#2}Assistant Professor Department of Computer science and Engineering
Bharathiyar Institute of Engineering For Women

Abstract—To date, the growth of automated personal data leads to a trend that data owners desire to slightly contract out their data to clouds for the enjoyment of the high-quality reclamation and storage service without worrying the affliction of local data management and conservation. However, secure share and search for the subcontracted data is a tough task, which may certainly incur the seepage of sensitive personal information. Efficient data sharing and searching with security is of perilous prominence. This paper, for the first time, proposes a searchable attribute-based proxy re-encryption system. When equated to surviving systems only supporting single functionality but, our new primitive supports both facilities and provides plastic keyword apprise service. Specifically, the system empowers a data owner to efficiently share his data to a detailed cluster of users matching a sharing policy and meanwhile, the data will retain its searchable assets but also the corresponding search keyword(s) can be updated after the data sharing. It is also proved elected ciphertext confident in the random oracle model.

Keywords: Searchable attribute-based encryption, keyword update, encrypted data sharing.

I. INTRODUCTION

By stepping into the period of big data, Internet users usually cherry-pick to upload their particular data to remote cloud servers such that they can diminish the cost of local data controlling and preservation. In tallying to personages, many industries and research institutions also monitor the trend to tenuously store commercial and scientific data to clouds to enjoy high speed data process and reclamation service. Cloud storage service, in view of that, reveals its infinite practical and commercial potential. However, it meanwhile compulsorily encounters with many erratic security and privacy challenges.

Motivation. We start with Attribute-Based Encryption (ABE) with a momentous reason that it provides fine-grained mournfulness in data share and search. After loading data to a cloud server, the data owner regularly needs two necessary operations: one is data searching, and the further is data distribution.

Leveraging out-dated ABE machinery to encrypt data that guarantees the secrecy of the data, but it restricts data distribution and penetrating. Suppose there is a set of genome encryption, which are donated by unknown volunteers for medical research persistence, where a data g_i is encrypted under a policy P_i such that only a group of researchers matching the policy can acquire the data. The ciphertexts are stored in a remote server. To trustingly search a specific encrypted genomic data, a researcher, says Alice, has to download all the ciphertexts related to her decryption policy P_A from the server, and next to decrypt them to fulfill the search task locally. When sharing one of her accessible data with her contemporaries, Alice has to download the encrypted data, decrypt and further re-encrypt it under the decryption policy of the contemporaries. Another interesting behavior, which might be done by Alice, is the keyword apprise for the mutual encoded data. Consider an encrypted genomic data is with a keyword tag ("Materials at Lab A"). After its distribution to scientists in Lab B, Alice may choose to change its tag as ("Shared to Lab B"). Since out-dated ABE cannot sustain keyword apprise, Alice has to modify the tags for all shared ciphertexts on her own due to defending the secrecy of the keywords. However, the above naive approaches do not scale well. Because they bring surplus



required to be on-line all the time. The cost for the data owner will become more burdensome, when the number of penetrating and partaking data is increasing. Moreover, the size of download data yields an encounter for local data preservation that definitely reduces the benefit of remote data storage. On the other hand, one may allow a (remote) third party to achieve data search task, the re-encryption of data and keyword update on behalf of Alice. Nonetheless, this requires the party to be fully trusted as it is established knowledge of search keyword (i.e. what Alice requirements to quest) and given the secret key of Alice (i.e. knowing the underlying data). The outflow of the above information earnestly disgraces the privacy of anonymous donors because the genomic data may contain profound information, such as illness. Therefore, this approach is also objectionable due to hurt of secrecy and concealment.

From the above considerations, we can see the significance of secure thorough and sharing for encrypted data in remote cloud storage scenario. Protecting the seclusion of search (including data and keyword) but also supporting efficient encrypted data distribution in the framework of ABE that is an exciting and unsolved problem in the nonfiction. This persuades our work. We further show some present primitives cannot fully solve the open problem.

Attribute-Based Keyword Search (ABKS). To hide quest contents as well as search keywords from cloud server, introduced the belief of Municipal Key Encryption (PKE) with keyword search, in which a user delivers a special token linked with keyword(s) to the server such that the server can practise the token to apportion all encoded data with the same keyword(s). The server, still, knows nil about the keyword(s) and the data. To notice the notion into the framework of ABE, Zheng, Xu and Ateniese defined ABKS.

Granting is the most recent work in the nonfiction of PKE with keyword search, it fails to support translated data sharing as the only way for a server to convert a given ciphertext to another one is to find the agreeing secret key, i.e. reading the primary data.

Attribute-Based Proxy Re-Encryption (ABPRE).

To resourcefully share a converted data with others, introduced PRE whereby a semi-trusted proxy can convert an encryption of a message to another encryption of the same message without knowing the message.

To employ the belief into ABE setting, proposed the notion of ABPRE. Recently, announced new types of ABPRE with solid refuge. Nonetheless, these systems cannot reach our goals as they do not succeed to pay for privacy-preserving keyword exploration.

Gaps Between ABE Keyword Pursuit and Data Stake.

Usually, an ABKS supportive keyword search does not concurrently deliver decryption service. This is due to a technical limitation in the assembly method of trapdoor token (used for searching). Unambiguously, a trapdoor token consists of a user's "re-randomized" secret key. By using this evidence, the token container (i.e. a cloud server) can simply get better the data from a ciphertext encoded under the decryption policy identical the key. While the server may use the re-randomized secret key to realize data distribution, the concealment of the data cannot be fail-safe.

On the other hand, an ABPRE system is not compatible with secure data search. Definitely, if we regard a feature as a search keyword, the seclusion of the keyword cannot be achieved as the system is built in the attribute freely known model. One valour question that if we can power prevailing unspecified ABE systems, such as, to fill the gaps here. Nonetheless, it is unknown that if we can engagement unspecified ABE practice to yield both data share and search as well as keyword privacy.

Our paper focuses on tackling the elusive gaps by recommending a fresh ABE system backup keyword sequestered search and converted data distribution separately.

A. Our Contributions

Official Roadmap. We choose an ABE system with fast decryption as a starting point. The reason of employing ABE is that ABE can afford mournfulness for data share and keyword search compared to other encryption systems. To



achieve the solitude of keyword search, we first extend the actual ABE system into the irregular pairings group. Under the possessions of disproportionate couplings, one cannot tell whether a given ciphertext holds a keyword or not even he can make pairing subtractions from the ciphertext apparatuses. This principle is similar with the technique of unknown Identity-Based Encryption (IBE). We state that the renovation also brings better effectiveness. We further allow a token related to a keyword to be fabricated via an interface between Private Key Generator (PKG) and a system user (who specifies the keyword). The erection of the token is somewhat similar to that of the secret key of the user. However, the token (related to a keyword) will not empower its frame (i.e. a cloud server) to decrypt the ciphertext associated with the same keyword. This is a necessary obligation for searchable encryption, i.e. a trapdoor token for a keyword cannot deliver decryption capability to cloud server.

To attain encrypted data distribution, we trust the resulting structure with the practice of ABPRE. The re-encryption is fiddly in the sense that we cover a secret key of a user with two haphazard reasons in the re-encryption key generation phase. One random factor is used to cover the partial decryption value of a ciphertext so that a server cannot gain familiarity of data by using this intermediate value and for now, the random factor is known only by a group of valid deputies with apposite decryption rights. The other random factor is used to hide the machineries of the secret key such that its acquaintance will not be escaped to the server.

Our gifts are defined as surveys.

- We, for the first time, familiarise a novel and practical notion, searchable ABPRE. Our notion guarantees that the keyword search facility of a ciphertext can be remained after the sharing of the ciphertext. It is wealth stating that all prevailing public key organizations with keyword search fail to promise this possessions.
- We enterprise a tangible searchable Key-Policy (KP) ABPRE system supporting the above notion. We also prove the scheme chosen ciphertext secure in the Random Oracle Model (ROM). The scheme is the first of its kind supporting the

privacy of keyword examination but also encoded data sharing.

- As of independent interest, our protocol supports keyword apprise so that a ciphertext's keyword can be extra updated already the ciphertext is shared with others. This property brings a handiness to data owner (who can gain admittance to the data) in the sense that the ciphertext keyword can be freely modified based on data share record.
- Our system has better efficiency regarding to keyword search and decryption phases when equated to prevailing systems which only funding either data sharing or keyword search in the context of ABE.

B. Related Work

Sahai and Waters introduced the notion of ABE. After that, Goyal et al. proposed a KP-ABE system, in which ciphertexts are concomitant with points, and secret keys are associated with access policies (over attributes). Later on, many classic ABE systems and their variants that have been proposed in the literature, introduced the first (keyword) Searchable Encryption (SE) system, in which full text search over encrypted data is allowable. Following the notion, many SE systems have been proposed. The existing systems can be categorized into two types: searchable symmetric key encryption and Searchable Public Key Encryption (SPKE). This paper deals with the latter case.

The PKE with single keyword search. Proposed an encryption mechanism supporting conjunctive keyword search. a more expressive keyword search encryption for not only conjunctive but also keyword subset/range queries. an efficient but deterministic searchable encryption. Particular deviations of SPKE have been wished-for in the literature, such as authorized keyword search and verifiable keyword exploration.

Newly, familiarized ABKS, in which they combine the keyword search with ABE technology. Nevertheless, none of the aforementioned SPKE systems supports encrypted data sharing.

Following the concept of decryption rights delegation, PRE is classified as: unidirectional and bidirectional PRE, and single-hop and multi-hop PRE. Our exertion transactions with the single-hop unidirectional delegation. Since the introduction



many works of PRE have been introduced. To combine PRE with ABE, introduced Ciphertext-Policy (CP) ABPRE, and construed a system on top of system. proposed another system providing strategy through AND gates on multi-valued and adversarial traits. proposed a CP-ABPRE scheme which is a bridge for ABE and IBE. proposed an obfuscation for functional re-encryption with collusion resistant property. Recently, a new CP-ABPRE was proposed, in which the scheme is proven in the ROM. a CP-ABPRE system was built and proven secure in contradiction of Select Ciphertext Dose (CCA) in the standard model. a more expressive CP-ABPRE with adaptively CCA security was constructed based on deterministic finite automata. However, the previously introduced systems cannot provide privacy-preserving keyword search.

We compare this work with the most recent SPKE scheme and ABPRE system in terms of functionality and security. We leave the efficiency comparison to the best of our knowledge, our scheme is the first to reach (privacy preserving)

keyword pursuit and encrypted data sharing as well as keyword update. Our system is based on asymmetric decisional 1-BDHE assumption, while on decisional linear assumption and some composite order group assumptions, respectively.

Trapdoor Generation. In our system, the keyword trapdoor is generated via the collaboration between a fully trusted PKG and a secret key holder. When the key holder needs a trapdoor, he first issues the corresponding request (with keyword(s)) to the PKG, the PKG then returns a related intermediate component. Finally, the key holder re-randomizes the component to become a “real” trapdoor. In our current architecture, we assume all master secret keys (the one for secret key generation, and the other one for trapdoor generation) are known by the PKG only. That is why the secret key holder needs a interaction with the PKG when generating a trapdoor. The system can be extended to allow a secret key holder to generate a trapdoor on his own without any help of PKG. This requires the secret key holder to know namely, is chosen by the secret key holder as one of his secret information.

We will regard the extension as one of future works.

REFERENCE

- 1) C. Wang, N. Cao, K. Ren, and W. Lou. Enabling secure and efficient ranked keyword search over outsourced cloud data. *IEEE Trans. Parallel Distrib. Syst.*, 23(8):1467–1479, 2012.
- 2) B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, editors, *Public Key Cryptography*, volume 6571 of LNCS, pages 53–70. Springer, 2011.
- 3) Y. Zhang, X. Chen, J. Li, D. S. Wong, and H. Li. Anonymous attribute-based encryption supporting efficient decryption test. In K. Chen, Q. Xie, W. Qiu, N. Li, and W. Tzeng, editors, *8th ACM Symposium on Information, Computer and Communications Security, ASIA CCS '13*, Hangzhou, China - May 08 - 10, 2013, pages 511–516. ACM, 2013.
- 4) Q. Zheng, S. Xu, and G. Ateniese. VABKS: verifiable attribute based keyword search over outsourced encrypted data. In *2014 IEEE Conference on Computer Communications, INFOCOM 2014*, Toronto, Canada, April 27 - May 2, 2014, pages 522–530. IEEE, 2014.
- 5) S. Hohenberger and B. Waters. Attribute-based encryption with fast decryption. In K. Kurosawa and G. Hanaoka, editors, *Public-Key Cryptography - PKC 2013 - 16th International Conference on Practice and Theory in Public-Key Cryptography*, Nara, Japan, February 26 - March 1, 2013. *Proceedings*, volume 7778 of *Lecture Notes in Computer Science*, pages 162–179. Springer, 2013.
- 6) K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T. V. X. Phuong, and Q. Xie. A dfa-based functional proxy re-encryption scheme for secure public cloud data sharing. *IEEE Transactions on Information Forensics and Security*, 9(10):1667–1680, 2014.
- 7) K. Liang, M. H. Au, W. Susilo, D. S. Wong, G. Yang, and Y. Yu. An adaptively cca-secure ciphertext-policy attribute-based proxy re-encryption for cloud data sharing. In X. Huang and J. Zhou, editors, *Information Security Practice and Experience - 10th International Conference, ISPEC 2014*, Fuzhou, China, May 5-8, 2014.



- Proceedings, volume 8434 of Lecture Notes in Computer Science, pages 448–461. Springer, 2014.
- 8) K. Liang, C. Chu, X. Tan, D. S. Wong, C. Tang, and J. Zhou. Chosen-ciphertext secure multi-hop identity-based conditional proxy re-encryption with constant-size ciphertexts. *Theor. Comput. Sci.*, 539:87–105, 2014.
 - 9) K. Liang, L. Fang, W. Susilo, and D. S. Wong. A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security. *In INCoS*, pages 552–559. IEEE, 2013.
 - 10) K. Liang, Q. Huang, R. Schlegel, D. S. Wong, and C. Tang. A conditional proxy broadcast re-encryption scheme supporting timed release. In R. H. Deng and T. Feng, editors, *ISPEC*, volume 7863 of *Lecture Notes in Computer Science*, pages 132–146. Springer, 2013.
 - 11) K. Liang, J. K. Liu, D. S. Wong, and W. Susilo. An efficient cloud-based revocable identity-based proxy re-encryption scheme for public cloud data sharing. In M. Kutyłowski and J. Vaidya, editors, *Computer Security-ESORICS 2014 - 19th European Symposium on Research in Computer Security*, Wroclaw, Poland, September 7–11, 2014. *Proceedings, Part I*, volume 8712 of *Lecture Notes in Computer Science*, pages 257–272. Springer, 2014.
 - 12) K. Liang, Z. Liu, X. Tan, D. S. Wong, and C. Tang. A CCA-secure identity-based conditional proxy re-encryption without random oracles. In T. Kwon, M.-K. Lee, and D. Kwon, editors, *ICISC*, volume 7839 of *LNCS*, pages 231–246. Springer, 2012.