Journal of Applied Information Science
9 (1) 2021, 26-29
http://www.publishingindia.com/jais

An Efficient and Expressive Keyword Search over Encrypted Data in Cloud for Data Security

V. Bhuvaneswari
Seshachala Degree & P.G. College, Puttur, Andhra Pradesh, India.

Abstract: Accessible encryption permits a cloud server to direct catchphrase search over encoded information for the benefit of the information clients without learning the basic plaintexts. In any case, most existing accessible encryption conspires just help single or conjunctive watchword search, while a couple of different plans that can perform an expressive catchphrase search are computationally wasteful since they are worked from bilinear pairings over the composite-request gatherings. Right now, propose an expressive open key accessible encryption plot in the prime-request gatherings, which permits catchphrase search arrangements (i.e., predicates, get to structures) to be communicated in conjunctive, disjunctive or any monotonic Boolean recipes and accomplishes huge execution improvement over existing plans. We officially characterize its security and demonstrate that it is specifically secure in the standard model. Additionally, we execute the proposed plot utilizing a fast prototyping device called Charm and direct a few examinations to assess its execution. The outcomes show that our plan is substantially more proficient than the ones worked over the composite-request gatherings [1, 2].

Keywords: Catchphrase, Computationally, Encryption, Learning, Secure.

I. Introduction

Cloud storage has drawn research attention in the last few years with the development of cloud computing. There are some IT systems providing storage services such as Dropbox, iCloud and SkyDrive, and more and more users are getting used to storing and accessing their data by smartphones in cloud storage. For the protection of privacy and confidentiality of sensitive data, secure encryption is an effective way to defend against attackers. A user has to encrypt these kinds of data before uploading them to a server. In the future, he may require to want a part of the encrypted data, but cannot reveal his key to the server. The user recalls all of them from the server and picks which part he really needs since the encrypted data are unreadable as random strings, which implies that the server cannot directly search with his requirement. In this scenario, how to obtain encrypted data therefore becomes a new security issue with regard to cloud storages over encrypted data. Data as a Service (DaaS), as the main function of cloud computing, provides an assurance that data is provided on-demand to a user regardless of the geographic or organizational separation of provider and consumer. To reduce costs and promote efficiency, organizations have been focusing on outsourcing their storage and computing needs currently. In DaaS, Public Key Encryption with Keyword Search (PEKS), as a fundamental searchable encryption component in Public Key Infrastructure (PKI), is efficient to both safeguard outsourced data (through encryption) and provide operability over encrypted data. Hence, PEKS has been introduced to eliminate secure concern in DaaS environment. The most urgent difficulty today in developing secure cloud computing is not promoting the efficiency of a kind of secure algorithm. Rather, it is the enhancement and optimization of infrastructure to support widespread and practical functions [3, 4]. In the existing Internet and cloud environment with an unlimited resource, it is intractable to manage certificates in PKI. Moreover, in a resource-constrained environment (such as Internet of Things, mobile network, et al), it becomes an impossible mission. Suppose such a scene: Alice is a bank manager, and she is on a vacation. She mails address, et al. It reduces the cost of certificate management through binding participant's identity and public key. Because the Private Key Generator (PKG) holds all the participants' key pairs inherently, it leads to key escrow problem. Once PKG is compromised, sensitive information of users will be revealed completely along with the private key. It severely restricts the promotion of PKI including PEKS component. Furthermore, most of the proposed PEKS schemes so far were established on IBC with key escrow problem inherently. Cloud sharing and E-mail system are the two most typical applications of DaaS in which search ability is indispensable. In the following contents,

E-mail system is as the application to illustrate our presentation. There are two physical entities in the E-mail system, client and server. Further, the client is divided into two logical entities, sender and receiver. Note that sender and receiver are seldom online simultaneously. Sender sends mails to Receiver and retrieves mails from the server. Server stores and manages the mails for all clients. When requesting mails for the receiver, he sends a keyword "unread" to server. Server will transmit the mails of "unread" receiver wants.

II. Key Policy Attribute-Based Encryption (KPABE)

Information encryption is the best as to keeping delicate information from unapproved get to. In prior open key encryption or personality-based encryption frameworks, scrambled information is focused on unscrambling by a solitary known client. To address these developing needs, Sahai and Waters [4] presented the idea of quality-based encryption (ABE). As an option of encoding to singular clients, in ABE framework, one can install an entrance strategy into the figure content or decoding key. Henceforth, information gets to is self-upholding from the cryptography, requiring no confided in go-between. ABE can be seen as an augmentation of the thought of personality-based encryption in which client character is summed up to a lot of expressive properties rather than a solitary string determining the client personality. Contrasted and personality-based encryption ABE has a noteworthy preferred position that it accomplishes adaptable one-to numerous encryptions as a substitute of balanced; it is imagined as a promising device for tending to the issue of secure and fine-grained information sharing and decentralized access control. There are two sorts of ABE relying upon which of private keys or figure messages that get to approaches are related with. KP-ABE is an open key cryptography crude for one-to numerous correspondences. In KP-ABE, records are related to properties for everyone of which an open key part is characterized [5]. The encode or partners the arrangement of ascribes to the message by scrambling it with the comparing open key segments. For every client an entrance structure is appointed, which is normally characterized as an entrance tree over information qualities, i.e., inward hubs of the entrance tree are edge entryways and leaf hubs are related with traits. Client mystery key is characterized to mirror the entrance structure so the client can decode a figure content if and just if the information qualities fulfill his entrance structure KP-ABE plans are appropriate for organized associations with rules about who may peruse specific reports. In a figure content arrangement quality-based encryption (CP-ABE) framework [9], when a sender encodes a message, they determine a particular access strategy as far as access structure over characteristics in the figure content, expressing what sort of recipients will have the option to unscramble the figure content. Clients have sets of properties and acquire relating mystery trait keys from the characteristic position. Such a client can unscramble a figure content if his/her characteristics fulfill the entrance strategy related to the figure content. Along these lines, CP-ABE component is thoughtfully nearer to prior job-based access control strategy [8].

III. Related Work

We can classify the current conjunctive watchword accessible plans into two sorts: the fixed catchphrase field and the variable watchword field. The fixed catchphrase field plans depend on the suspicion which recognizes m watchword fields for each record. At the point when the recipient produces the trapdoor, he needs to distinguish the watchword handle that he needs to look [6]. It is not hard to apply since the inquiry framework can be actualized like a social database the board framework; that is, the point at which the client wishes to look through the information, he can enter the watchwords as per the fields that the framework sets. In another hand, the variable watchword field plans can be applied to more than the social database. The benefit of variable watchword field is that it just needs the less measure of the extra room for the server to store the figure content. On the off chance that the extra room is an on-request stockpiling administration, the client can just buy the negligible extra room [7]. On the difference, the fixed watchword field has the benefit of security and comfort since it uncovers minimal measure of data to the server. Be that as it may, so as to plan a conjunctive watchword accessible plan which is reasonable for the vast majority of the applications, Park *et al.* introduced another plan dependent on an open key cryptosystem, which is named Public key Encryption with Conjunctive fields Keyword Search (PECKS) plot. They utilized the fixed catchphrase field's presumption and embraced the bilinear matching to develop their plan. Be that as it may, by un et al. called attention to that PEKS plan might be assaulted effectively by disconnected watchword speculating assaults since the catchphrase space is a lot littler than the secret word. Plus, the trapdoors are moved by means of an open system in the plan depends on the open key cryptosystem the assailants have a lot of likelihood to spy the trapdoors and get the watchwords from them. Hence, the greater part of the current catchphrase accessible plans pays more considerations on upgrading the security of their plans. Sadly, some of the plans need a lot of registering time or produce long watchword figure writings and trapdoors which are wasteful for clients.

Right now, build a proposed plot dependent on bilinear pairing and talk about the prerequisites as follows:

- *Enforceability of the Trapdoor*: Since the watchword figure writings contain the recipient's open key, just the trapdoor which is produced by the relating private key can finish the questions. In this way, the proposed plan ought to guarantee that nobody can produce legitimate trapdoor without the approved beneficiary's private key.

- *Anonymousness of the Figure Content*: After scrambling, the watchwords are changed into a consecutive of characters that cannot be recognized. This necessity implies that no one can pick up the inserted watchwords from the catchphrase figure writings.
- *Practicability*: For clients, it is oppressive to recollect an excessive amount of additional data to scramble the catchphrases and search the encoded information. In this way, the proposed plan ought to be embraced effectively in the truth.
- *Efficiency:* Most of the current conjunctive catchphrase accessible plans are as yet wasteful for clients. So as to apply the conjunctive catchphrase accessible plan with frail gadgets, the proposed plan ought to perform effectively.
- *Against Disconnected Catchphrase Speculating Assaults*: Since the trapdoors are moved in the open system, the foes can without much of a stretch catch the trapdoors. Nonetheless, the trapdoors should make sure about enough that can remain against within and outside disconnected catchphrase speculating assaults.

IV. Proposed System

A. Correctness

Alice runs the Key Gen algorithm to generate her public/private key pair. She uses Trapdoor to generate trapdoors Tw for any keywords w that she wants the mail server or mail gateway to search for. The mail server uses the given trapdoors as input to the Test algorithm to determine whether a given email contains one of the keywords w specified by Alice. Let positive integer N be the product of two k-bit (k is the security parameter), distinct odd primes p, q. Let e be a randomly chosen positive integer less than and relatively prime to $\varphi(N) = (p - 1)(q - 1)$. Then the encrypted e-mail e M m returned to Alice, Alice could use her private key to decrypt the e-mail like $M^d = m$. In conclusion, our scheme is correct.

B. Security in Proposed System

Our scheme provides provable secrecy for encryption, the e-mails are encrypted by the standard RSA encryption scheme, there are no feasible means to decrypt. The encrypted e-mails without the private key d. So, the mail server cannot get any information about the content of the e-mails. What is more, our scheme provides query isolation, all the computations in the PKES scheme are performed in an encrypted way, so, the mail server learns nothing more about the plaintext than the search result. Our scheme also provides controlled searching, the trapdoors are generated by using the secret key of the receiver, so, without knowing the secret of the receiver, the mail server cannot search an arbitrary keyword. Because of the secrecy of the secret key, there is no a more efficient way to forge a trapdoor than factoring the modulus N. As we all know, when the modulus is big enough, it is very hard to factor it. Finally, our scheme provides hidden queries, so that the user may ask the untrusted mail server to search for a keyword without revealing the keyword to the mail server. In our scheme, every time the user wants to search for a keyword, she will choose a random integer, without knowing $\varphi(N)$, it is hard for the mail server to compute an inverse of an integer. Based on the hardness of the discrete logarithm problem, it is hard to compute the random integer r from r s, so the mail server gets no information of the keyword during the searching process. To avoid reply attacking, the user may sign the trapdoor using a secure signature. In conclusion, our PKES scheme is secure.

C. Performance

In our scheme, the public parameters are a modulus, two integers and a hash function; the private keys are several integers and a modulus. To generate the keys in the scheme, we can refer the methods to save computation time and space. The encryption of the keywords and the data are using two exponent arithmetic computations. When a user generates the trapdoors, only an integer multiplication and an exponent computation are need. And we note that the random integer r and the exponent computation can be done offline, thus the users can take full advantage of their device. In our Test operation, only an exponent and a comparison between two integers are needed. In a word, all the computations in our scheme are basic arithmetic, when comparing with the schemes which use a lot of pair computation, our scheme is more efficient.

V. Conclusion

In order to allow a cloud server to search on encrypted data without learning the underlying plaintexts in the public key setting, Boneh proposed a cryptographic primitive called public-key encryption with keyword search (PEKS). Since then, considering different requirements in practice, e.g., communication overhead, searching criteria and security enhancement, various kinds of searchable encryption systems have been put forth. However, there exist only a few public-key searchable encryption systems that support expressive keyword search policies, and they are all built from inefficient composite-order groups. In this paper, we focused on the design and analysis of public-key searchable encryption systems in the prime-order groups that can be used to search multiple keywords in expressive searching formulas. Based on a large universe key-policy attribute-based encryption scheme given in, we presented an expressive searchable encryption system in the prime order group which supports expressive access

structures expressed in any monotonic Boolean formulas. Also, we proved its security in the standard model and analyzed its efficiency using computer simulations.

References

[1] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions," *J. Cryptology*, vol. 21, no. 3, pp. 350-391, 2008.

[2] J. Baek, R. Safavi-Naini, and W. Susilo, "On the integration of public key data encryption and public key encryption with keyword search," In ISC*, LNCS,* vol. 4176, pp. 217-232, Springer, 2006.

[3] M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and efficiently searchable encryption," In CRYPTO, *LNCS*, vol. 4622, pp. 535-552, Springer, 2007.

[4] S. Benabbas, R. Gennaro, and Y. Vahlis, "Verifiable delegation of computation over large datasets," In CRYPTO, *LNCS*, vol. 6841, pp. 111-131, Springer, 2011.

[5] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano. "Public key encryption with keyword search," In EUROCRYPT, *LNCS*, vol. 3027, pp. 506-522, Springer, 2004.

[6] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," In *INFOCOM'14*, IEEE, Piscataway, NJ, USA, 2014, pp. 2112-2120.

[7] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," In *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1. pp. 222-233, 2014.

[8] C. Bosch, Q. Tang, P. H. Hartel, and W. Jonker, "Selective document retrieval from encrypted database," In ISC, *LNCS*, vol. 7483, pp. 224-241, Springer, 2012.

[9] J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy, "Blind and anonymous identity-based encryption and authorised private searches on public key encrypted data," In PKC, *LNCS*, vol. 5443, pp. 196-214, Springer, 2009.