An Efficient And Expressive Keyword Search Over Encrypted Data In Cloud For Data Secuirity

Jujjavarapu Kusuma Rathnam#1, S.Chittibabulu#2
1Student, Computer Science and Engineering, NOVA College of Engineering and Technology, Vegavaram(V), Jangareddigudem(M) West Godavari(D) Andhra Pradesh
2Guide, Associate Professor, Computer Science and Engineering NOVA College of Engineering and Technology, Vegavaram(V), Jangareddigudem(M) West Godavari(D) Andhra Pradesh

Abstract_ Searchable encryption allows a cloud server to conduct keyword search over encrypted data on behalf of the data users without learning the underlying plaintexts. However, most existing searchable encryption schemes only support single or conjunctive keyword search, while a few other schemes that are able to perform expressive keyword search are computationally inefficient sincethey are built from bilinear pairings over the composite-order groups. In this paper, we propose an expressive public-key searchable encryption scheme in the prime-order groups, which allows keyword search policies (i.e., predicates, access structures) to be expressed in conjunctive, disjunctive or any monotonic Boolean formulas and achieves significant performance improvement over existing schemes. We formally define its security, and prove that it is selectively secure in the standard model. Also, we implement the proposed scheme using a rapid prototyping tool called Charm [37], and conduct several experiments to evaluate it performance. The results demonstrate that our scheme is much more efficient than the ones built over the composite-order groups.

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 smart phones in cloud storage. For the protection of privacy and confidentiality of sensitive data, secure encryption is an effective way to defense against attackers. A user has to encrypt these kinds of data before uploading them to a server. In the future, he may require 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 a main function of cloud computing, provides an assurance that data is provided on demand to user regardless of 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. In existing Internet and cloud environment with unlimited resource, it is intractable to manage certificates in PKI. Moreover, in resource-constrained environment (such as internet of Things, mobile network, et al), it becomes an impossible mission. Suppose such scene: Alice is a bank manager, and she is on a vacation. She mail address, et al. It reduces the cost of certificate management through binding participant's identity and public key. Because 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 proposed PEKS schemes so far were established on IBC with key escrow problem inherently. Cloud sharing and E-mail system are 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 E-mail system, client and server. Further 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 server. Server stores and manages the mails for all clients. When requesting mails for receiver, he sends a keyword "unread" to server. Server will transmit the mails of "unread" receiver wants.

II.KEY POLICY ATTRIBUTE-BASED ENCRYPTION (KPABE)

Data encryption is the most effective in regard to preventing sensitive data from unauthorized access. In earlier public key encryption or identity-based encryption systems, encrypted data is targeted for decryption by a single known user. To address these emerging needs, Sahai and Waters [4] introduced the concept of attribute-based encryption (ABE). As an alternative of encrypting to individual users, in ABE system, one can embed an access policy into the cipher- text or decryption key. Hence, data access is self-enforcing from the cryptography, needing no trusted mediator. ABE can be viewed as an extension of the notion of identity-based encryption in which user identity is generalized to a set of expressive attributes instead of a single string specifying the user identity. Compared with identity-based encryption ABE has significant advantage that it achieves flexible one-to many encryption as a substitute of one-to-one; it is envisioned as a promising tool for addressing the problem of secure and fine-grained data sharing and decentralized access control. There are two types of ABE depending on which of private keys or cipher texts that access policies are associated with. KP-ABE is a public key cryptography primitive for one-to many communications. In KP-ABE, files are associated with attributes for each of which a public key component is defined [5]. The encrypt or associates the set of attributes to the message by encrypting it with the corresponding public key components. For each user an access structure is assigned, which is usually defined as an access tree over data attributes, i.e., inner nodes of the access tree are threshold gates and leaf nodes are associated with attributes. User secret key is defined to reflect the access structure so that the user is able to decrypt a cipher text if and only if the data attributes satisfy his access structure KP-ABE schemes are suitable for structured organizations with rules about who may read particular documents. In a cipher text-policy attribute-based encryption (CP-ABE) system [9], when a sender encrypts a message, they specify a specific access policy in terms of access structure over attributes in the cipher text, stating what kind of receivers will be able to decrypt the cipher text. Users possess sets of attributes and obtain corresponding secret attribute keys from the attribute authority. Such a user can decrypt a cipher- text if his/her attributes satisfy the access policy associated with the cipher text. Thus, CP-ABE mechanism is conceptually closer to earlier role-based access control method [18].

III. RELATED WORK

We can categorize the existing conjunctive keyword searchable schemes into two types: the fixed keyword field and the variable keyword field. The fixed keyword field schemes are based on the assumption which identifies m keyword fields for each document. When the receiver generates the trapdoor, he has to identify the keyword fields that he wants to search. It is not difficult to apply since the query system can be implemented like a relational database management system; that is, when the user wishes to search the data, he can input the keywords according to the fields that the system sets. In another hand, the variable keyword field schemes can be applied to more than the relational database. The advantage of variable keyword field is that it only needs the less amount of the storage space for the server to store the cipher text. If the storage space is an on demand storage service, the user can only purchase the minimal storage space. On the contrast, the fixed keyword field has the advantage of security and convenience because it reveals the least amount of information to the server. However, in order to design a conjunctive keyword searchable scheme which is suitable for most of the applications, Park et al. presented a new scheme based on a public key cryptosystem, which is named Public key Encryption with Conjunctive fields Keyword Search (PECKS) scheme. They used the fixed keyword field's assumption and adopted the bilinear pairing to construct their scheme. However, By un et al. pointed out that PEKS scheme may be attacked easily by off-line keyword-guessing attacks since the keyword space is much smaller than the password. Besides, the trapdoors are transferred via a public network in the scheme based on the public key cryptosystem the attackers have much probability to eavesdrop the trapdoors and derive the keywords from them. Therefore, most of the existing keyword searchable schemes pay more attentions on enhancing the security of their schemes.

Unfortunately, some of schemes need a large amount of computing time or produce long keyword cipher texts and trapdoors which are inefficient for users.

In this paper, we construct a proposed scheme based on bilinear paring and discuss the requirements as follows:

1. Enforceability of the trapdoor: Since the keyword cipher texts contain the receiver's public key, only the trapdoor which is generated by the corresponding private key can complete the queries. Therefore, the proposed scheme should ensure that no one can forge the legal trapdoor without the authorized receiver's private key.

2. Anonymousness of the cipher text: After encrypting, the keywords are changed into a sequential of characters that cannot be distinguished. This requirement means that nobody can gain the embedded keywords from the keyword cipher texts.

3. Practicability: For users, it is burdensome to remember too much extra information to encrypt the keywords and search the encrypted data. Therefore, the proposed scheme should be adopted easily in the reality.

4. Efficiency: Most of the existing conjunctive keyword searchable schemes are still inefficient for users. In order to apply the conjunctive keyword searchable scheme with weak devices, the proposed scheme should perform efficiently.

5. against off-line keyword-guessing attacks: Since the trapdoors are transferred in the public network, the adversaries can easily capture the trapdoors. However, the trapdoors should secure enough that can stand against the inside and outside off-line keyword-guessing attacks.

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's 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's more, our scheme provides query isolation, all the computations in the PKES scheme are performed in a 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's 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's very hard to factoring 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 φ(N), it's hard for the mail server to compute an inverse of a integer. Based on the hardness of the discrete logarithm problem, it's 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, user may sign the trapdoor use 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 ur scheme, we can refer the methods to save the 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 a integer multiplication and a 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 uses 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 publickey 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 the 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.

VI.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, 21(3):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, vol. 4176 of LNCS, pp. 217–232. Springer, 2006.

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

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

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

[6]. Wang B, Yu S, Lou W, Hou T (2014) Privacy-Preserving Multi-Keyword Fuzzy Search over Encrypted Data in the Cloud. In: INFOCOM'14. IEEE, Piscataway, N.J, USA. pp 2112–2120

[7]. Cao N, Wang C, Li M, Ren K, Lou W (2014) Privacy-preserving multi-keyword ranked search over encrypted cloud data. In: IEEE Transactions on Parallel and Distributed Systems. IEEE, Piscataway, N.J, USA Vol. 25, no. 1. pp 222–233

[8] C. Bosch, Q. Tang, P. H. Hartel, and W. Jonker. Selective document ¨ retrieval from encrypted database. In ISC, vol. 7483 of LNCS, 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, vol. 5443 of LNCS, pp. 196–214. Springer, 2009.

Author's Details:

Jujjavarapu Kusuma Rathnam Studying M.Tech (2nd year Pursuing) Computer Science and Engineering.

S.Chittibabulu Working as Associate Professor Qualification:M.Tech(Ph.D)