International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 15
May 2018

Expressive And Effective Public-Key Searchable Encryption Scheme Over Encrypted Data Of Cloud Store In The Prime-Order Groups

khatijatul kubra and Md Ateeq Ur Rahman [2],

[1]*Research Scholar, Dept. of Computer Science & Engineering,*

SCET, Hyderabad, India

shadan.16081d8203@gmail.com

[2]*Professor and Head, Dept. of Computer Science & Engineering,*

SCET, Hyderabad, India

shadan.authors1@gmail.com

Abstract - Searchable cryptography permits a cloud server to conduct keyword search over encrypted information on behalf of the information users while not learning the underlying plaintexts. However, most existing searchable cryptography schemes solely support single or conjunctive keyword search, whereas a number of different schemes that square measure ready to perform communicatory keyword search square measure computationally inefficient since they're engineered from additive pairings over the composite-order teams. during this paper, we tend to propose associate communicatory public-key searchable cryptography theme within the prime-order teams, that permits keyword search policies (i.e., predicates, access structures) to be expressed in conjunctive, divisional or any monotonic Boolean formulas and achieves vital performance improvement over existing schemes. we tend to formally outline its security, and prove that it's by selection secure within the normal model. Also, we tend to implement the projected theme employing a speedy prototyping tool known as Charm , and conduct many experiments to judge it performance. The results demonstrate that our theme is way a lot of economical than those engineered over the composite-order teams.

Index Terms—Searchable encryption, cloud computing, expressiveness, attribute-based encryption.

I. INTRODUCTION

Consider a cloud-based aid data system that hosts outsourced personal health records (PHRs) from varied aid suppliers. The PHRs ar encrypted so as to suits privacy rules like HIPAA. so as to facilitate information use and sharing, it's extremely fascinating to own a searchable coding (SE) theme that permits the cloud service supplier to look over encrypted PHRs on behalf of the approved users

(such as medical researchers or doctors) while not learning data regarding the underlying plaintext. Note that the context we have a tendency to ar considering supports non-public information sharing among multiple information suppliers and multiple information users. Therefore, SE schemes within the private-key setting, that assume that one user United Nations agency searches and retrieves his/her own information, don't seem to be appropriate. On the opposite hand, non-public data retrieval (PIR) protocols, which permit users to retrieve a precise information-item from a information that in public stores data while not revealing the data-item to the information administrator, are not appropriate, since they need the info to be in public offered.

In order to tackle the keyword search drawback within the cloud-based aid data system situation, we have a tendency to resort to public-key coding with keyword search (PEKS) schemes, that is first projected in. in an exceedingly PEKS theme, a ciphertext of the keywords known as "PEKS ciphertext" is appended to Associate in Nursing encrypted PHR. To retrieve all the encrypted PHRs containing a keyword, say "Diabetes", a user sends a "trapdoor" related to asearch question on the keyword "Diabetes" to the cloud service supplier, that selects all the encrypted PHRs containing the keyword "Diabetes" and returns them to the user whereas while not learning the underlying PHRs. However, the answer in in addition as different existing PEKS schemes that improve on solely support equality queries .

Set intersection and meta keywords1, will be used for conjunctive keyword search. However, the approach supported set intersection leaks further data to the cloud server on the far side the results of the conjunctive question, while the approach exploitation meta keywords need 2m meta keywords to accommodate all the potential conjunctive queries for m keywords.

In order to deal with the higher than deficiencies in conjunctive keyword search, schemes like those in, were argue within the public-key setting. Ideally, within the sensible applications, search predicates (i.e., policies) ought to be communicatory specified they'll be expressed as conjunction, disjunction or any mathematician formulas2 of keywords. within the higher than cloud-based aid system, to seek out the connection between polygenic disorder and age or weight, a medical scientist might issue an exploration question with Associate in Nursing access structure (i.e., predicate) ("Illness = Diabetes" AND ("Age = 30" OR "Weight = 150-200")). SE schemes supporting communicatory keyword access structures were conferred in. sadly, the theme in has exponentially increasing quality , whereas the schemes in ar supported the inefficient additive pairing over composite-order teams [17]. although there exist techniques [17] to convert pairing-based schemes from composite-order teams to prime-order teams, there's still a major performance degradation thanks to the one. Meta keywords ar composed of many keywords. For example, a document that contains the keywords "Bob", "urgent" and "finance" could also be increased with the meta-keyword "Bob: urgent: finance" two. during this paper, unless otherwise mere, the mathematician formulas we have a tendency to mention ar monotonic. That is, they contains solely AND and OR gates, let's say, A AND (B OR C). needed size of the special vectors [18].

In this paper, we have a tendency to propose a public-key based mostly communicatory SE theme in prime-order teams, that is very appropriate for keyword search over encrypted information in situations of multiple information house

owners and multiple information users like the cloud-based aid data system that hosts outsourced PHRs from varied aid suppliers.

II. Related Works

Public cloud service suppliers give associate degree infrastructure that offers businesses and people access to computing power and cupboard space on a pay-as-you-go basis. this permits these entities to bypass the standard prices related to having their own information centre such as: hardware, construction, air-con and security prices, as an instance, creating this an economical answer for information storage. If the info being keep is of a sensitive nature, encrypting it before outsourcing it to a public cloud could be a smart technique of guaranteeing the confidentiality of the info. With the info being encrypted, however, looking out over it becomes impossible. during this paper, we tend to examine totally different architectures for supporting search over encrypted information and discuss a number of the challenges that require to be overcome if these techniques area unit to be built into sensible systems.

Nowadays, the majority information is keep digitally. Public cloud service suppliers give associate degree infrastructure that offers businesses and people access to computing power and cupboard space to support this digital information on a versatile pay-as-you-go basis. this permits them to bypass the prices related to having their own information centres corresponding to hardware, construction, air-con and security prices. This makes cloud computing a really efficient answer for each bulk processing and information storage. in keeping with a government survey on info security and information breaches with reference to digital information in 2015 [1], ninety p.c of huge organisations were attacked by associate degree unauthorised outsider and suffered a knowledge breach that year (up from eighty one p.c the previous year). tiny businesses, that were antecedently not a serious target, were conjointly reportage increased attacks, with the quantity of those businesses attacked in 2015 rising by fourteen p.c from the previous year. furthermore because the increase in variety of information breaches occurring, the monetary prices to corporations of those breaches, as an instance, thanks to business disruption, loss of sales and compensation, was conjointly shown to own up. This demonstrates a transparent want for secure information storage so as to make sure the confidentiality of information. However, encrypting information is simply one a part of the answer. Encrypting information ensures that, within the event of a compromise, no significant info ought to leak concerning the info itself if the info is compromised, however it conjointly reduces the likelihood of playing computations on the ciphertexts, corresponding to looking for keywords or specific things among the info. Suppose that, even as in an exceedingly typical cloud storage surroundings, your information is keep in encrypted type on a distant server thanks to native information storage constraints. To find a bit of information, we tend to may transfer the whole thing of the encrypted information, decrypt it, and search over the unencrypted information. or else, maybe we tend to may produce associate degree index for the encrypted information that's keep domestically and accustomed navigate the encrypted files. each of those strategies give adequate solutions in theory, yet, in apply, they gift

many issues. Firstly, the dimensions of the encrypted information might not be renowned a priori, or be renowned prior to to be terribly giant, each of that hold the method of downloading all of the encrypted information extremely inefficient and expensive. what is more, the rationale for storing the info remotely within the 1st place is thanks to the inconvenience of native storage, thus downloading all the info during this case wouldn't be associate degree choice. making associate degree index would need domestically storing a file which can be of a size within the order of the quantity of encrypted files, that once more isn't possible thanks to native storage restrictions. additionally, the index itself may doubtless leak info concerning the encrypted information, compromising confidentiality. Searchable encoding (SE) provides an answer to the current downside by supporting the outsourcing of encrypted information to a distant server, while maintaining the power to look for specific keywords among the encrypted information. The literature concerning SE is extensive; but, SE isn't wide deployed in apply. This chapter identifies and analyses totally different situations to that SE may be applied within the universe and investigates the suitableness of sure styles of SE schemes to every situation. we tend to conjointly explore the explanations on why SE schemes don't seem to be wide enforced and appearance at the protection problems and practicality of protocols that area unit presently being enforced that succeed some type of search over encrypted information. during this work, we tend to analyze sensible situations involving access to encrypted information and appearance at ways in which SE may well be accustomed solve issues among these situations. once analyzing the situations, we tend to checked out options corresponding to the quantity of users, the adversarial threat, sensitivity of {the information|the info|the information} concerned and whether or not static or dynamic data is employed, and assessed the suitableness of explicit SE schemes to every situation. we tend to used this analysis to outline four basic situations to that SE may well be applied supported the quantity of users and also the capabilities of every user. among every of those basic situations, we tend to determine varied options of the situations that occur within the universe. we tend to then map specific SE schemes into the various instances of the situation looking on the varied options. there's a comprehensive survey of incontrovertibly secure searchable encoding schemes that post dates our initial analysis that may be found here [2]. They follow the same categorization of SE schemes; but, this survey takes a theoretical approach and doesn't contemplate the sensible reasons behind the categorisation of the SE schemes. we tend to don't shall give a comprehensive survey of each SE theme so far, and also the intention here is to explore what options of associate degree SE theme would possibly build it a lot of appropriate to be used in an exceedingly explicit situation so as to facilitate the look of protocols that use SE to produce solutions to real-world issues. the remainder of this text is unionized as follows: in Section two, we tend to outline the system and adversarial models for SE. Section three defines the four situations and analyzes the SE schemes within the literature, mapping them into these four situations in keeping with numerous options of the schemes. Section four appearance at SE schemes that area unit designed specifically to be deployed within the universe and discusses their numerous strengths and weaknesses. Section five appearance at many factors that area unit preventing the readying of SE.

2.1 Existing System

In a private-key SE setting, a user uploads its personal information to an overseas info and keeps the info personal from the remote info administrator. Private-key SE permits the user to retrieve all the records containing a specific keyword from the remote info. However, because the name suggests, private-key SE solutions solely apply to eventualities wherever information house owners and information users entirely trusty one another.

Private info Retrieval. With regard to public info cherish stock quotes, wherever the user is unaware of it and needs to go looking for a few data-item while not revealing to the info administrator that item it's, personal info retrieval (PIR) protocols were introduced, which permit a user to retrieve information from a public info with way smaller communication then simply downloading the complete info. withal, in our context, the info isn't in public obtainable, the info isn't public, therefore the PIR solutions cannot be applied.

Disadvantages:
Private-key SE solutions solely apply to eventualities wherever information house owners and information users entirely trusty one another.
Nevertheless, in our context, the info isn't in public obtainable, the info isn't public, therefore the PIR solutions can not be applied..

III. PROPOSED SYSTEM

We propose a public-key primarily based communicative SE theme in prime-order teams, that is very appropriate for keyword search over encrypted information in eventualities of multiple information house owners and multiple information users akin to the cloud-based care data system that hosts outsourced PHRs from numerous care suppliers.

Our communicative SE theme consists of a trusty trapdoor generation center that publishes a public system parameter and keeps a passkey on the Q.T., a cloud server that stores and searches encrypted information on behalf of knowledge users, multiple information house owners World Health Organization transfer encrypted information to the cloud, and multiple information users World Health Organization would love to retrieve encrypted information containing bound keywords. To source AN encrypted document to the cloud, an information owner appends the encrypted document with keywords encrypted below the general public parameter and uploads the combined encrypted document and encrypted keywords to the cloud. To retrieve all the encrypted documents containing keywords satisfying a particular access structure (i.e., predicate or policy) akin to (“Illness = Diabetes” AND (“Age = 30” OR “Weight = 150- 200”)), an information user 1st obtains a trapdoor related to the access structure from the trapdoor generation center so sends the trapdoor to the cloud server. The latter can conduct the search and come the corresponding encrypted documents to the info user.

IV. System Architecture

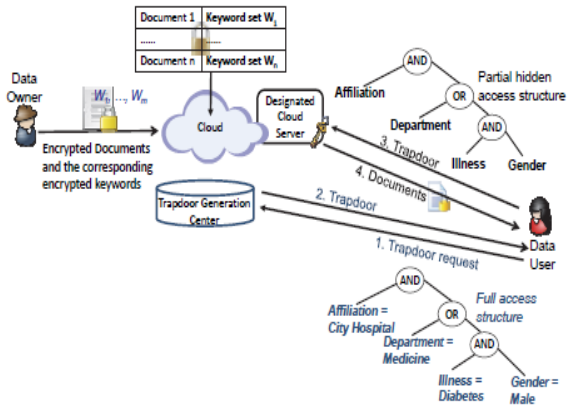

Figure 1: System Architecture of the Proposed System

The design of our SE system is shown in Fig. 1, that consists of 4 entities: a trusty trapdoor generation centre World Health Organization publishes the system parameter and holds a master personal key and is to blame for the trapdoor generation, knowledge homeowners World Health Organization transfer the encrypted knowledge to a public cloud, knowledge users World Health Organization ar privileged to go looking and access the encrypted knowledge, and a chosen cloud server World Health Organization executes the keyword search operations for knowledge users. To modify the cloud server to go looking over ciphertexts, the info homeowners append each encrypted document with encrypted keywords4. a knowledge user problems a trapdoor request by causing associate access structure over keywords to the trapdoor generation centre that generates and returns a trapdoor such as the access structure. we have a tendency to assume that the trapdoor generation centre contains a separate authentication mechanism to verify every knowledge user so issue them the corresponding trapdoors. once getting a trapdoor, the info user sends the trapdoor with a corresponding partial hidden access structure (i.e., the access structure while not keyword values) to the selected cloud server. The latter performs the testing operations between every ciphertext and also the trapdoor victimisation its personal key, and forwards the matching ciphertexts to the info user.

As mentioned earlier, a ciphertext created by a knowledge owner consists of the encrypted document generated victimisation associate secret writing theme and also the encrypted keywords generated victimisation our SE theme. From currently on, we have a tendency to solely think about the latter a part of the encrypted document, and ignore the primary half since it's out of the scope of this paper. In summary, the planning goals of our communicative SE theme ar fourfold. eight quality. The planned theme ought to support keyword access structures expressed in any mathematician formula with AND and OR gates. eight potency. The planned theme ought to be adequately economical in terms of computation, communication and storage for sensible applications. eight Keyword privacy. First, a ciphertext while not its corresponding trapdoors mustn't disclose any data concerning the keyword values it contains to the cloud server and outsiders. Second, a trapdoor mustn't leak data on keyword values to any outside attackers while not the personal key of the selected cloud server. we have a tendency to capture the linguistics security for the SE theme to confirm that encrypted knowledge doesn't reveal any data concerning the keyword values, that we have a tendency to decision "selective sameness against chosen keyword-set attack (selective IND-CKA security)" (See Appendix A). eight obvious security. the protection of the planned theme ought to be formally evidenced below the quality model instead of the informal analysis.

v. CONCLUSION

In order to permit a cloud server to go looking on encrypted information while not learning the underlying plaintexts within the publickey setting, Boneh projected a cryptologic primitive known as public-key coding with keyword search (PEKS). Since then, considering totally different needs in observe,e.g., communication overhead, looking criteria and security sweetening, numerous varieties of searchable coding systems are place forth. However, there exist solely a number of public-key searchable coding systems that support communicatory keyword search policies, and that they square measure all designed from the inefficient composite-order teams . during this paper, we have a tendency to targeted on the look and analysis of public-key searchable coding systems within the prime-order teams which will be wont to search multiple keywords in communicatory looking formulas. supported an outsized universe key-policy attribute-based coding theme given in [18], we have a tendency to given associate degree communicatory searchable coding system within the prime order cluster that supports communicatory access structures expressed in any monotonic Boolean formulas. Also, we have a tendency to proven its security within the commonplace model, and analyzed its potency exploitation laptop simulations.

References

[1] O. Goldreich and R. Ostrovsky, "Software protection and simulation
on oblivious rams," J. ACM, vol. 43, no. 3, pp. 431–473, 1996.
[2] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for
searches on encrypted data," in 2000 IEEE Symposium on Security
and Privacy, Berkeley, California, USA, May 14-17, 2000. IEEE
Computer Society, 2000, pp. 44–55.
[3] E. Goh, "Secure indexes," IACR Cryptology ePrint Archive, vol.
2003, p. 216, 2003.
[4] C. Cachin, S. Micali, and M. Stadler, "Computationally private
information retrieval with polylogarithmic communication," in
Advances in Cryptology - EUROCRYPT '99, International Conference
on the Theory and Application of Cryptographic Techniques, Prague,
Czech Republic, May 2-6, 1999, Proceeding, ser. Lecture Notes in
Computer Science, vol. 1592. Springer, 1999, pp. 402–414.
[5] G. D. Crescenzo, T. Malkin, and R. Ostrovsky, "Single database private
information retrieval implies oblivious transfer," in Advances
in Cryptology - EUROCRYPT 2000, International Conference on the
Theory and Application of Cryptographic Techniques, Bruges, Belgium,
May 14-18, 2000, Proceeding, ser. Lecture Notes in Computer Science,
vol. 1807. Springer, 2000, pp. 122–138.
[6] W. Ogata and K. Kurosawa, "Oblivious keyword search," J. Complexity,
vol. 20, no. 2-3, pp. 356–371, 2004.
[7] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public
key encryption with keyword search," in Advances in Cryptology
- EUROCRYPT 2004, International Conference on the Theory and
Applications of Cryptographic Techniques, Interlaken, Switzerland, May
2-6, 2004, Proceedings, ser. Lecture Notes in Computer Science, vol.
3027. Springer, 2004, pp. 506–522.
[8] J. Lai, X. Zhou, R. H. Deng, Y. Li, and K. Chen, "Expressive
search on encrypted data," in 8th ACM Symposium on Information,

Computer and Communications Security, ASIA CCS '13, Hangzhou,
China - May 08 - 10, 2013. ACM, 2013, pp. 243–252.
[9] P. Golle, J. Staddon, and B. R. Waters, "Secure conjunctive keyword
search over encrypted data," in Applied Cryptography and
Network Security, Second International Conference, ACNS 2004, Yellow
Mountain, China, June 8-11, 2004, Proceedings, ser. Lecture Notes in
Computer Science, vol. 3089. Springer, 2004, pp. 31–45.
[10] D. J. Park, K. Kim, and P. J. Lee, "Public key encryption with conjunctive field keyword search," in Information Security Applications,5th International Workshop, WISA 2004, Jeju Island, Korea, August 23-25, 2004, Revised Selected Papers, ser. Lecture Notes in Computer Science, vol. 3325. Springer, 2004, pp. 73–86.