ISSN : 2347 - 2243

Indo - American Journal of Life Sciences and Biotechnology

www.iajlb.com
Email : editor@iajlb.com or iajlb.editor@gamil.com

Indo-Am. J. of LifeSc & Bt.,2022- *ISSN 2347-2243 www.iajlb.com*

Indo-American Journal of Life Sciences and Biotechnology

Vol.19, Issue.2, May 2022

EFFICIENT AND EXPRESSIVE KEYWORD SEARCH OVER ENCRYPTED DATA IN CLOUD

1G.CHANDRIKA,2K.VENKATESH

ABSTRACT:

For information customers, searchable encryption means that a cloud server can do keyword searches over encrypted data without obtaining the core plain texts. However, the vast majority of publicly available encryption schemes only allow for a single or conjunctive keyword search, while the few schemes that allow for an expressive keyword search are computationally inefficient. For the purposes of communicating policy strategies using conjunctive, disjunctive, or monotonic Boolean equations, we present an expressive open key accessible encryption conspire in prime-arrange gatherings in this paper. In the standard model, we demonstrate that it is explicitly secure and present it in a formal way. We also use Charm, a rapid prototyping tool, to put the recommended strategy into action and run a few tests to see how well it works. It's clear from the results that our plan is more effective than the ones that were used for composite-order groups.

KEYWORDS:proving security; encrypting using a public key; searching for keywords

I.INTRODUCTION

With the rise of cloud computing, cloud storage has become a hot topic in academia. More and more people are storing and accessing their data in cloud storage via their smartphones thanks to systems like Dropbox, iCloud, or SkyDrive. Secure encryption is an effective defense against attackers when it comes to protecting sensitive data. Encryption is required before uploading this type of data to a server. When he needs to decrypt a portion of the encrypted material, he can't give the server his key since he doesn't trust the server. As soon as the user receives them all from the server, he or she can pick and choose which section they

Because the server cannot immediately search with his request, random strings are unintelligible. It becomes a new security concern in this scenario when it comes to cloud storages and encrypted data.

DaaS, a primary feature of cloud computing, ensures that data is available to users independent of geographic or organizational separation between supplier and consumer. Currently, enterprises are

1M.Techstudent,DeptofCSE,RamachandraCollegeof engineering,Eluru,India
2AssistantProfessor,DeptofCSE, Ramachandracollegeofengineering,Eluru,India
reallyneeds,sincetheencrypteddataare

focused on outsourcing their storage and computing requirements in order to cut costs and improve productivity. PEKS, as a key searchable encryption component in Public Key Infrastructure (PKI), is effective in DaaS for both the protection of externally supplied data (via encryption) and the operation of encrypted data. In order to eliminate security concerns in a DaaS context, PEKS was developed. In establishing safe cloud computing, the most pressing issue today involves the development of a secure algorithm that is both efficient and effective. As a matter of fact, infrastructure improvement and optimization are the primary goals. The management of Public Key Infrastructure (PKI) certificates has become impossible in today's Internet and cloud environments, where resources are virtually limitless. As a result, in resource-constrained environments like the Internet of Things, mobile networks, etc., it is an impossible job.Alice, a bank manager, is on vacation, thus this scenario might play out: She

II. It is possible that she would prefer to get her e-mails on a variety of devices, including her laptop and mobile phone. She may want the mail server to send urgent e-mails to her mobile phone, and other e-mails to her laptop, depending on her preferences. A trapdoor "urgent" must be sent to the mail server by Alice in order to accomplish this purpose. As a result, the mail server can scan through the e-mails and distribute them to other devices. Emails may be encrypted before being sent by Alice due to the relevance and privacy of their content. Traditional public key encryption algorithms might be used by the senders to encrypt the keywords with Alice's public key, and Alice could also use her public key to generate a trapdoor if she so chose. The mail server might then perform a comparison between the emails' contents and any encrypted keywords. Although it's possible that if Alice generates a trapdoor using her public key, anyone could do the same. As a result, Alice's private key should only be used to generate the trapdoors. Traditional public key encryption algorithms may not be appropriate for encrypting keywords in light of these considerations. This issue can be solved with public key encryption and keyword search. The mail server may determine which e-mails should be sent to the laptop or mobile device by computing the trapdoor and the encrypted keyword combined. Now-a-days, cloud storage has become an essential method of data storage. It is possible to use the cloud storage server as a mail server. It is, however, important to point out that there are no operational PKES schemes based on bilinear maps. The inefficiency of PKES in cloud storage may be the most difficult issue to overcome. As a result of our work, we have developed a very safe and efficient public key encryption system that uses factoring, which is incredibly efficient.

III. A participant's public key can be derived from his unique identifier, such as a mobile phone number or e-mail address, using Identity-Based Cryptography (IBC).

IV. mail-to address, etc. Certificate administration costs are reduced by tying participants' identities and public keys together. Key escrow is a concern since the Private Key Generator (PKG) maintains all of the participants' key pairs. There will be no way to recover the private key or any other sensitive information once PKG has been compromised. Including the PEKS component, it severely restricts PKI's marketing. The majority of current PEKS schemes are based on IBC, which introduces a key escrow issue by design. DaaS applications that rely on search include cloud storage and e-mail systems, two of the most common. As an example, we'll use an email

system to demonstrate our point in the following sections. Clienandserverarthe two physical components that make up an email system. Sender and receiver are two separate logical entities within the client. Senders and receivers are rarely online at the same time. Messages are sent and received by the Sender and the Receiver. Email is stored and managed centrally by the server, serving as a single point of access for all users. Receiver sends the phrase "unread" to the server while requesting mails for the receiver. The server will send the "unread" recipient's mails if they request it.

VI. BACKGROUND

The fundamental security of an encryptionscheme requires it to provide privacy forto decrypt the information Popular formalizations, such as distinguish ability (semantic security) or non-malleability, are commonly used to meet a variety of data privacy needs. Attacks can be targeted at either plaintext or a variety of specified cipher text types. To ensure the encoded information is safe, an encryption scheme requires a strong key security. Various kinds of information protection requirements necessitate the coordination of notable formalizations, such as in recognize capacity (semantic security) or non-flexibility, under either picked plaintext or different kinds of picked figure content attacks. Whatever the case may be,

Encryption strategies aren't designed solely for the purpose of securing information. Lately, the safety of customers has been of equal concern, which motivates an investigation network to seek out anonymity features when developing cryptographic natives. Encryption, known as "beneficiary secrecy" or "key security," was first introduced in the open key encryption environment with the goal of obscurity, and then it was introduced to the personality-based setting with the goal of obscurity.

In most cases, a sender and a recipient are included in a two-party convention when examining data security and key protection. It has becoming increasingly common for outsiders to be used in cryptography natives, and this has become an important part of modern data security. It's a common question to ask how to ensure security assurance if outsiders use cryptography frameworks. Private key generators in character-based settings, for example, are entirely trusted in some systems. It's possible that an outsider may not be fully fair because of this presumption, but it's impossible to say for sure. This dilemma can be avoided by confiding in an outsider to a limited extent rather than fully. Numerous cryptographic conventions, such as server-aided frameworks, have taken this more reasonable concern into account.Then again, the foes in the security ideasunder the established security models areexpected to have no entrance to the privatekeys. Be that as it may, this is illogical ingenuine frameworks, as a rule the foe maygetsomehalfwaydataaboutthekeysthrought echniqueswhicharenotforeseen

by the framework's creator and, as a result, not taken into account when arguing for its protection. It has been shown that the enemy can use physical side-channels to reveal fractional information about the internal conditions of program executions through continuing planning or to use blame injection systems to interfere with and prompt alterations to the gadget's internal condition. Assaults known as key-swapping assaults come in a wide variety. This perspective raises the question of how to maintain safety and achieve security in cryptography under difficult circumstances.

VII. Various security approaches, such as spillage-safe cryptography, semantic security for wiretap channels, and cryptography secure against related-key assaults and alteration, have been proposed to address this issue. It is hypothesized that a related-key attack, in which an adversary alters an equipment put away key and then observes the cryptographic crude's yield under the new key, might compromise the security of a small number of cryptographic natives. Because these clients don't claim information, it's imperative that they keep their data safe. Various expert checking conventions,

referred to as evidence of irretrievability, have been proposed to allow information trustworthiness to be checked without completely downloading the information, with the goal of reducing the misuse of correspondence transfer speed caused by the downloading of a large amount of information just to check its trustworthiness. There are techniques that can protect these frameworks from related-key attacks, which we study in this proposal.

VIII. RELATEDWORK

We may divide existing conjunctive keyword searching schemes into two categories: those that use fixed keywords and those that use variable keywords. Based on this idea, fixed keyword field schemes have been implemented.

For each page, this identifies m keyword fields. Trapdoors can only be opened if the receiver knows what keywords he wants to seek. A relational database management system can be used to construct a query system, so the user can enter keywords into the system's fields when he or she searches for information. On the other hand, the variable keyword field schemes can be used in relational databases as well as other types of databases. The benefit of using a variable keyword field is that the server needs to keep the cipher text in a less amount of space. The user can only acquire the bare minimum of storage capacity if it is an on-demand storage service. While the variable keyword field is more convenient, it also provides more security because it divulges less information to the server.

However, Park et al. presented a novel method based on a public key cryptosystem named Public key Encryption with Conjunctive fields Keyword Search (PECKS) in order to design a conjunctive keyword searchable scheme that is suited for the majority of applications. They built their technique on the assumption of a fixed keyword field and the bilinear pairing. PEKS, on the other hand, is vulnerable to off-line keyword guessing attacks since the keyword space is less than the password's password-guessing area. A public network and a public key cryptosystem make it easier for attackers to spy on the trap doors and extract the keywords from them, making the scheme vulnerable to eavesdropping. As a result, the majority of currently implemented keyword searchable methods place a higher priority on security. Schemes that require a substantial amount of processing time or produce long keyword cipher texts and trapdoors that are inefficient for end-users are a drawback.

According to the requirements outlined in this research, we suggest a bilinear paring technique.

As a result of the receiver's public key being encoded as a keyword cipher text, the trapdoor generated by that receiver's private key can only finish queries. If someone attempts to fake the legal trapdoor, they will need the authorized receiver's private key to do it.

Second, the cipher text is completely anonymous: The keywords are transformed into a sequence of characters that cannot be deciphered. No one can decipher the keyword cipher texts and decode the contained keywords because of this stipulation.

IX.For users, encrypting keywords and searching encrypted data is time-consuming and difficult. In practice, the recommended plan should be straightforward.

X.The majority of existing conjunctive keyword searching methods are still inefficient for the end-users. The proposed method must perform well in order to make the conjunctive keyword searching scheme usable with weak devices.

XI.to prevent keyword-guessing attacks that take place offline: Having the trapdoors in the public network makes it easy for the adversary to get their hands on them. In order to protect against off-line keyword guessing assaults from both within and outside, the trapdoors must be sufficiently secure.

PROPOSEDSYSTEM

a) Correctness

To create her public and private key pair, Alice uses the Key Gen algorithm. When she wants

the mail server or mail gateway to search for specific keywords, Trapdoor generates trapdoors Tw for those keywords using the Trapdoor API. Using the trapdoors as input to the Test method, the mail server can assess whether an email contains one of the keywords w defined by Alice. ' Letpositive integer N be the product of two k-bit(kisthesecurityparameter),distinct

b) p and q are the odd primes. Give us an odd positive integer, say, less than or roughly equal to e(N), which is both smaller and more prime than N. After receiving the encrypted e-mail e M m, Alice was able to decrypt the e-mail using her private key. Finally, we can say that our strategy is sound.

c) SecurityinProposedsystem

The e-mails are encrypted using the usual RSA encryption algorithm, and there is no practical way to decrypt them. The private key d is missing from the encrypted emails. As a result, the mail server is unable to access any information regarding e-mail messages' content. As an additional benefit, our PKES technique provides query isolation, which means that the mail server learns nothing more about plaintext than the search result from the PKES scheme. Our system also allows for controlled searching; the trapdoors are constructed using the receiver's secret key, so the mail server cannot search for an arbitrary keyword without knowing the receiver's secret. Trapdoors can only be forged by factoring the modulus N because of the secret key's secrecy. Factoring a large modulus is notoriously difficult, as we've all learned. When searching for a keyword, the user can ask an untrusted mail server to do so without revealing it to the mail server. In our system, the user selects a random integer each time she wishes to search for a term, which makes it difficult for the mail server to compute the inverse of an integer. A random integer r can't be generated from r s because of the difficulty of solving the discrete logarithm issue, hence no keyword information is retrieved throughout the search process. The user has the option of signing the trapdoor with a secure signature in order to avoid reply attacks. Finally, we can say that our PKES system is safe.

d) Performance

In our scheme, the public parameters are amodulus,twointegersandahashfunction; Several numbers plus a modulus make up the private key. To reduce time and space, we can use the methods to create the keys in our scheme. Data and keywords are encrypted using arithmetic computations that use two exponents. Integer multiplication and an exponent computation are all that's required for creating the trapdoors. We also point out that the random number r and the exponent computation can be done offline, allowing the user to take full advantage of their device's capabilities. Only an exponent and a comparison of two numbers are required in our Test procedure. Simply expressed, our method is more efficient than other schemes that rely on pair computation since all of its calculations are based on basic arithmetic.

XII. CONCLUSION

Public-key encryption with keyword search was proposed by Boneh in order to allow a cloud server to search encrypted data without knowing the underlying plaintexts in the publickey setup (PEKS). Since then, numerous types of searchable encryption systems have been proposed in consideration of various practical requirements, such as communication overhead, search criteria, and security enhancement. While some public-key searchable encryption systems provide expressive keyword search rules, most are based on inefficient composite-order group constructions. For the sake of searching multiple terms in expressive search formulas, we studied public-key searchable encryption systems in the prime-order groups in this study. An expressive searchable encryption system in the prime order group, based on a large-universe key-policy attribute-based encryption technique, provides expressive access structures defined in any monotonic Boolean formulas. Using computer simulations, we were

able to demonstrate its security and evaluate its performance.

XIII. REFERENCES

[1]O.ACM J. 43(3):431–473, Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious rams."

[2](2) "Practical approaches for searches on encrypted data," at the IEEE Symposium on Security and Privacy 2000, Berkeley, California, USA, May 14-17, 2000, D.X. Song D. Wagner A. Perrig [2] IEEE Computer Society, 2000, pages 44–55.

[3] IACR Cryptology ePrint Archives, 2003, vol. 2003, p. 216, 2003.

[4] "Computationally private information retrieval with polylogarithmic communication," in Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of the Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding, ser. Lecture Notes in Computer Science, vol. 1592." Page numbers 402–414 are from Springer (1999).

[5] In Advances in Cryptology - EUROCRYPT 2000 International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceedings, ser. Lecture Notes in Computer Science, vol. 1807. [5] G. D. Crescenzo, T. Malkin and R. Ostrovsky "Oblivious transfer implies a single database private information retrieval." Published in 2000 by Springer, pp. 122–138,

[6]Oblivious keyword search, by Ogata and K. Kurosawa, in J. Complexity, 20(2), 356–371.

[7]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.J.Lai,X.Zhou,R.H.Deng,Y.Li,and K. Chen, “Expressive search on encrypteddata,”in8thACMSymposiumonInformation, Computer &Communications Security, ASIA CCS '13, Hangzhou, China - May 8 - 10, 2013. ACM, 2013, p. 243–252. ACM, 2013.

Confidential conjunctive keyword search over encrypted data is described in the proceedings of the Second International Conference on Applied Cryptography and Network Security (ACNS 2004, Yellow Mountain, China, June 8–11, 2004). As cited in Springer (2004, 31–45).

Public key encryption with conjunctive field keyword search, in 5th International Workshop, WISA 2004, Jeju Island, Korea, August 23-25, 2004, Revised Selected Papers, series: Lecture Notes in Computer Science, vol. 3325, D. J. Park, K. Kim, and P. J. Lee. 73–86.

A multi-user system for public key encryption with conjunctive keyword search was presented by Y. H. Hwang and P. J. Lee in Pairing 2007, a first international conference on pair-based cryptography held in Tokyo, Japan from July 2 to 4, 2007. The paper was published in Lecture Notes in Computer Science, series 4575. Pages 2–22 of Springer, 2007.

A conjunctive-subset keyword search for an efficient public key encryption is described in J. Network and Computer Applications, 34, no. 1, pp. 262–267 in 2011.