Dual-Server Public-Key Encryption with Keyword Search For Secure Cloud Storage

ENGINEERING IN ADVANCED RESEARCHSCIENCE AND TECHNOLOGY

ISSN 2352-8648
Vol.03, Issue.01
October-2021
Pages: -338-344

DUAL-SERVER PUBLIC-KEY ENCRYPTION WITH KEYWORD SEARCH FOR SECURE CLOUD STORAGE

[1] *M. Tech., Dept of CSE, Sri Sunflower College of Engineering And Technology. AP, India,* vallurivenkatalakshmi1@gmail.com
[2]*M. Tech., Dept of CSE, Sri Sunflower College of Engineering And Technology. AP, India,* laxmirtx@@gmail.com

Abstract:- Searchable encryption is of increasing interest for protecting the data privacy in secure searchable cloud storage. In this paper, we investigate the security of a well-known cryptographic primitive, namely, public key encryption with keyword search (PEKS) which is very useful in many applications of cloud storage. Unfortunately, it has been shown that the traditional PEKS framework suffers from an inherent insecurity called inside keyword guessing attack (KGA) launched by the malicious server. To address this security vulnerability the first thing is his/her secret key stored in the computer. The second thing is a unique personal security device which connects to the computer. It is impossible to decrypt the cipher text without either piece. More importantly, once the security device is stolen or lost, this device is revoked. It cannot be used to decrypt any cipher text. This can be done by the cloud server which will immediately execute some algorithms to change the existing cipher text to be un-decrypt able by this device. This process is completely transparent to the sender. Furthermore, the cloud server cannot decrypt any cipher text at any time. The security and efficiency analysis show that our system is not only secure but also practical.

Keywords-KGA,Cloud server,PEKS

I. INTRODUCTION:-

Cloud storage [4], [3], [9], [5], [10] is a model of networked storage system where data is stored in pools of storage which are generally hosted by third parties. There are many benefits to use cloud storage. The most notable is data accessibility. Data stored in the cloud can be accessed at any time from any place as long as there is network access. Storage maintenance tasks, such as purchasing additional storage capacity, can be offloaded to the responsibility of a service provider. Another advantage of cloud storage is data sharing between users. If Alice wants to share a piece of data (e.g. a video) to Bob, it may be difficult for her to send it by email due to the size of data. Instead, Alice uploads the file to a cloud storage system so that Bob can download it at anytime. Despite its advantages, outsourcing data storage also increases the attack surface area at the same time. For example, when data is distributed, the more locations it is stored the higher risk it contains for unauthorized physical access to the data. By sharing storage and networks with many other users it is also possible for other unauthorized users to access your data. This may be due to mistaken actions, faulty equipment, or sometimes because of criminal intent. A promising solution to offset the risk is to deploy encryption technology. Encryption can protect data as it is being transmitted to and from_ _Kaitai Liang is the corresponding author. _ J. K. Liu is with Monash University, Australia. E-mail: joseph.liu@monash.edu. _ K. Liang is with Aalto University, Finland. E-mail: kaitai.liang@aalto.fi. _ W. Susilo is with University of Wollongong, Australia. E-mail: wsusilo@uow.edu.au. _ J. Liu is with Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, China. E-mail: jianghualiu11@gmail.com. _ Y. Xiang is with the School of Information Technology, Deakin University, Australia. E-mail: yang@deakin.edu.au. the cloud service. It can further protect data that is stored at the service provider. Even there is an unauthorized adversary who has gained access to the cloud, as the data has been encrypted, the adversary cannot get any information about the plaintext. Asymmetric encryption allows the encryptor to use only the public information (e.g. public key or identity of the receiver) to generate a ciphertext while the receiver uses his/her own secret key to decrypt. This is the most convenient mode of encryption for data transition, due to the elimination of key management existed in symmetric

encryption. ENHANCED SECURITY PROTECTION. In a normal asymmetric encryption, there is a single secret key corresponding to a public key or an identity. The decryption of ciphertext only requires this key. The key is usually stored inside either a personal computer or a trusted server, and may be protected by a password. The security protection is sufficient if the computer/server is isolated from an opening network. Unfortunately, this is not what happens in the real life. When being connected with the world through the Internet, thecomputer/server may suffer from a potential risk that hackers may intrude into it to compromise the secret key without letting the key owner know. In the physical security aspect, the computer storing a user decryption key may be used by another user when the original computer user (i.e. the key owner) is away (e.g. when the user goes to toilet for a while without locking the machine). In an enterprise or college, the sharing usage of computers is also common. For example, in a college, a public computer in a copier room will be shared with all students staying at the same floor. In these cases, the secret key can be compromised by some attackers who can access the victim's personal data stored in the cloud system. Therefore, there exists a need to enhance IEEE Transactions on Computers,Volume:65,Issue:6, Issue Date :June.1.2016 2 the security protection. An analogy is e-banking security. Many e-banking applications require a user to use both a password and a security device (two factors) to login system for money transfer. The security device may display a one-time password to let the user type it into the system, or it may be needed to connect with the computer (e.g. through USB or NFC). The purpose of using two factors is to enhance the security protection for the access control. As cloud computing becomes more mature and there will be more applications and storage services provided by the cloud, it is easy to foresee that the security for data protection in the cloud should be further enhanced [7], [2], [12], [18]. They will become more sensitive and important, as if the e-banking analogy. Actually, we have noticed that the concept of two-factor encryption, which is one of the encryption trends for data protection1, has been spread into some real-world applications, for example, full disk encryption with Ubuntu system, AT&T two factor encryption for Smartphones2, electronic vaulting and druva - cloud-based data encryption3. However, these applications suffer from a potential risk about factor revocability that may limit their practicability. Note we will explain it later. A flexible and scalable two factor encryption mechanism is really desirable in the era of cloud computing. That motivates our work.

II. Related Work:-

Apply Key Words on Encrypted Data:-

There are generally three parties involved in communication model for a keyword search protocol. i.e. user, data owner and cloud server. The user is only data owner in the private cloud. But here the public cloud will be considered for most of the discussions involving three different parties by passing the keywords to the data owner the user initiates the search request. Then a trapdoor is sent to the cloud by the data owner to initiate the protocol for searching the keywords requested. With the indexes to the requested documents the cloud finally gives response to the user. There is more computational power in the cloud server when compared to the user and owner. Therefore the storage and computational cost will be placed on the cloud server.

Multi Key Word Search Over Encrypted Data:-

A diagram of our plans shows customer initially encodes the plaintext record; at that point the scrambled list is validated with our homomorphism MAC (Song *et al.* 2000) strategy, which produces confirmation labels for the scrambled list. Next, the file and verification labels are transferred to the cloud. By then the client can make an interest trapdoor created key, and uses our homomorphism MAC methodology to approve the trapdoor. With the confirmed trapdoor, the cloud server can homomorphically execute the interest work over the confirmation (Song et al. 2000) marks to deduce the result with a proof, which can confirm the question yield. Accept the chronicle set D to be redistributed contains N reports. For the I-th report, its sub record Di is worked as a n-dimensional piece vector spoke to as Di[j] is set to 1 if this document contains the j-the watchword in a given word reference; else, it is set as 0. In this way, the request Q is also a n- dimensional (Yang et al. 2011) piece vector, with the bits contrasting with the watchwords captivated by the client set to 1. By then the sub record Di and the request Q are encoded using cross section duplication, i.e., eDi = MTDi and eQ = M1Q where M is a genuine mystery network. The closeness score can even now be acquired through internal result of the encoded list and query,i.e. (MTDi)TM1Q = DT I Q. To cover the genuine comparability scores for more grounded protection, the report list and the inquiry vector can be stretched out with arbitrary numbers .Specifically, a record list is reached out to Di = (Di, i) 1),while the inquiry vector is reached out to ~Q = (rQ; r; t),

where I; r; t are irregular numbers and t is generally little. Finally, the last closeness score are processed by the cloud server will be r(Di, Q+_i)+t. Notwithstanding the way that the comparability score is randomized with the discretionary numbers, the cloud server is up 'til now prepared to rank the results without knowingreal scores. We apply our homomorphism MAC framework on the mixed rundown eDi and request eQ (trapdoor) to make check names for them, by then the cloud server homomorphically executes the multi-catchphrase (Fu et al. 2015) search work (interior thing) over the affirmation marks to procure the results. Since our homomorphism MAC strategy is adjusted to help tasks over genuine numbers, it underpins catchphrase search activities splendidly. Utilizing a single direction work, our homomorphism MAC strategy is profoundly productive in calculation. For each incentive in the scrambled record sub list and inquiry, verification labels are created as pursues. VP Search confirms everything (a genuine number) in the scrambled list eDi and inquiry eQ along with two coefficients of a degree- 1 polynomial. Evidence of watchword indexed lists is accomplished by homomorphically assessing the hunt work over the verification labels. The cloud server plays out the multi catchphrase search work, for example ascertaining The marking approach in our homomorphism MAC can adequately lessen extra room contrasted with self-assertively naming huge measure of information. Along these lines, the customer needs to register the worth f(FK(L1); :::; FK(Ln)) for confirmation generated each record. As the capacity f is lightweight, the confirmation can be performed productively.

III. Literature Survey:-

1) Privacy-assured outsourcing of image reconstruction service in cloud

AUTHORS: B. Zhang, J. Wang, K. Ren, and C. Wang

Large-scale image data sets are being exponentially generated today. Along with such data explosion is the fast-growing trend to outsource the image management systems to the cloud for its abundant computing resources and benefits. How to protect the sensitive data while enabling outsourced image services, however, becomes a major concern. To address these challenges, we propose outsourced image recovery service (OIRS), a novel outsourced image recovery service architecture, which exploits different domain technologies and takes security, efficiency, and design complexity into consideration from the very beginning of the service flow. Specifically, we choose to design OIRS under the compressed sensing framework, which is known for its simplicity of unifying the traditional sampling and compression for image acquisition. Data owners only need to outsource compressed image samples to cloud for reduced storage overhead. In addition, in OIRS, data users can harness the cloud to securely reconstruct images without revealing information from either the compressed image samples or the underlying image content. We start with the OIRS design for sparse data, which is the typical application scenario for compressed sensing, and then show its natural extension to the general data for meaningful tradeoffs between efficiency and accuracy. We thoroughly analyze the privacy-protection of OIRS and conduct extensive experiments to demonstrate the system effectiveness and efficiency. For completeness, we also discuss the expected performance speedup of OIRS through hardware built-in system design.

2) Fine-grained access control system based on outsourced attribute-based encryption

AUTHORS: J. Li, X. Chen, J. Li, C. Jia, J. Ma, and W. Lou

As cloud computing becomes prevalent, more and more sensitive data is being entralized into the cloud for sharing, which brings forth new challenges for outsourced data security and privacy. Attribute-based encryption (ABE) is a promising cryptographic primitive, which has been widely applied to design fine-grained access control system recently. However, ABE is being criticized for its high scheme overhead as the computational cost grows with the complexity of the access formula. This disadvantage becomes more serious for mobile devices because they have constrained computing resources. Aiming at tackling the challenge above, we present a generic and efficient solution to implement attribute-based access control system by introducing secure outsourcing techniques into ABE. More precisely, two cloud service providers (CSPs), namely key generation-cloud service provider (KG-CSP) and decryption-cloud service provider (D-CSP) are introduced to perform the outsourced key-issuing and decryption on behalf of attribute authority and users respectively. In order to outsource heavy computation to both CSPs without private information leakage, we formulize an underlying primitive called outsourced ABE (OABE) and propose several constructions with outsourced decryption and key-

issuing. Finally, extensive experiment demonstrates that with the help of KG-CSP and D-CSP, efficient key-issuing and decryption are achieved in our constructions.

3) Outsourcing encryption of attributebased encryption with mapreduce

AUTHORS: J. Li, C. Jia, J. Li, and X. Chen

Attribute-based encryption (ABE) is a promising cryptographic tool for fine-grained access control. However, the computational cost in encryption commonly grows with the complexity of access policy in existing ABE schemes, which becomes a bottleneck limiting its application. In this paper, we formulize the novel paradigm of outsourcing encryption of ABE to cloud service provider to relieve local computation burden. We propose an optimized construction with MapReduce cloud which is secure under the assumption that the master node as well as at least one of the slave nodes is honest. After outsourcing, the computational cost at user side during encryption is reduced to approximate four exponentiations, which is constant. Another advantage of the proposed construction is that the user is able to delegate encryption for any policy.

4) Secure and practical outsourcing of linear programming in cloud computing

AUTHORS: C. Wang, K. Ren, and J. Wang

Cloud computing enables customers with limited computational resources to outsource large-scale computational tasks to the cloud, where massive computational power can be easily utilized in a pay-per-use manner. However, security is the major concern that prevents the wide adoption of computation outsourcing in the cloud, especially when end-user's confidential data are processed and produced during the computation. Thus, secure outsourcing mechanisms are in great need to not only protect sensitive information by enabling computations with encrypted data, but also protect customers from malicious behaviors by validating the computation result. Such a mechanism of general secure computation outsourcing was recently shown to be feasible in theory, but to design mechanisms that are practically efficient remains a very challenging problem. Focusing on engineering computing and optimization tasks, this paper investigates secure outsourcing of widely applicable linear programming (LP) computations. In order to achieve practical efficiency, our mechanism design explicitly decomposes the LP computation outsourcing into public LP solvers running on the cloud and private LP parameters owned by the customer. The resulting flexibility allows us to explore appropriate security/efficiency tradeoff via higher-level abstraction of LP computations than the general circuit representation. In particular, by formulating private data owned by the customer for LP problem as a set of matrices and vectors, we are able to develop a set of efficient privacy-preserving problem transformation techniques, which allow customers to transform original LP problem into some random one while protecting sensitive input/output information. To validate the computation result, we further explore the fundamental duality theorem of LP computation and derive the necessary and sufficient conditions that correct result must satisfy. Such result verification mechanism is extremely efficient and incurs close-t- - o-zero additional cost on both cloud server and customers. Extensive security analysis and experiment results show the immediate practicability of our mechanism design.

5) Private and cheating-free outsourcing of algebraic computations

AUTHORS: D. Benjamin and M. J. Atallah

We give protocols for the secure and private outsourcing of linear algebra computations, that enable a client to securely outsource expensive algebraic computations (like the multiplication of huge matrices) to two remote servers, such that the servers learn nothing about the customer's private input or the result of the computation,and any attempted corruption of the answer by the servers is detected with high probability. The computational work done locally by the client is linear in the size of its input and does not require the client to carry out locally any expensive encryptions of such input.The computational burden on the servers is proportional to the time complexity of the current practically used algorithms for solving the algebraic problem (e.g., proportional to n3 for multiplying two ntimesn matrices). If the servers were to collude against the client,then they would only find out the client's private inputs, but they would not be able to corrupt the answer without detection by the client.

Proposed Algorithm:-

Hybrid Cipher text policy ABE Scheme with CCA We propose a solid circuit cipher text-arrangement characteristic based crossover encryption with certain assignment plan dependent on the multi linker maps and the undeniable processing innovation under cloud condition. We give a short portrayal of the convention Authority creates private keys for the information proprietor also, client. The information proprietor scrambles(Lin *et al.* 2017) his information utilizing mixture encryption framework, creates a secretly obvious Macintosh (Hong *et al.* 2015) for each symmetric cipher text and afterward transfers the entire cipher text to the cloud server. By then the data owner could be detached. The customer, who needs to access to the data, speaks with the cloud server. The ran jolts exhibit that the value is moved clandestinely, while the solid jolts show that the value is moved without an ensured channel Utilizing general circuits to communicate the passageway control Approach, we manufacture a monotone circuit with significance l and data size to be n.

IV. Conclusion:-

In this paper, we introduced a novel Dual-Server Public-Key Encryption with Keyword Search For Secure Cloud Storage , in which a data sender is allowed to encrypt the data with knowledge of the identity of a receiver only, while the receiver is required to use both his/her secret key and a security device to gain access to the data. Our solution not only enhances the confidentiality of the data, but also offers the revocability of the device so that once the device is revoked; the corresponding cipher text will be updated automatically by the cloud server without any notice of the data owner. Furthermore, we presented the security proof and efficiency analysis for our system.

V.REFERENCES:-

[1] A. Akavia, S. Goldwasser, and V. Vaikuntanathan. Simultaneous hardcore bits and cryptography against memory attacks. In TCC, volume 5444 of Lecture Notes in Computer Science, pages 474–495. Springer, 2009.

[2] S. S. Al-Riyami and K. G. Paterson. Certificateless public key cryptography. In ASIACRYPT, volume 2894 of Lecture Notes in Computer Science, pages 452–473. Springer, 2003.

[3] M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen. Certificate based (linkable) ring signature. In ISPEC, volume 4464 of Lecture Notes in Computer Science, pages 79–92. Springer, 2007.

[4] M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, and G. Yang. Malicious kgc attacks in certificateless cryptography. In ASIACCS, pages 302–311. ACM, 2007.

[5] M. Blaze, G. Bleumer, and M. Strauss. Divertible protocols and atomic proxy cryptography. In K. Nyberg, editor, EUROCRYPT, volume 1403 of LNCS, pages 127–144. Springer, 1998.

[6] A. Boldyreva, V. Goyal, and V. Kumar. Identity-based encryption with efficient revocation. In P. Ning, P. F. Syverson, and S. Jha, editors, ACM Conference on Computer and Communications Security, pages 417–426. ACM, 2008.

[7] D. Boneh, X. Ding, and G. Tsudik. Fine-grained control of security capabilities. ACM Trans. Internet Techn., 4(1):60–82, 2004.[8] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In CRYPTO '01, volume 2139 of LNCS, pages 213– 229. Springer, 2001.

[9] R. Canetti and S. Hohenberger. Chosen-ciphertext secure proxy re-encryption. In P. Ning, S. D. C. di Vimercati, and P. F. Syverson, editors, ACM Conference on Computer and Communications Security, pages 185–194. ACM, 2007.

[10] H. C. H. Chen, Y. Hu, P. P. C. Lee, and Y. Tang. Nccloud: A network-coding-based storage system in a cloud-of-clouds. IEEE Trans. Computers, 63(1):31–44, 2014.

[11] S. S. M. Chow, C. Boyd, and J. M. G. Nieto. Security-mediated certificateless cryptography. In Public Key Cryptography, volume 3958 of Lecture Notes in Computer Science, pages 508–524. Springer, 2006.

[12] C.-K. Chu, S. S. M. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng. Key-aggregate cryptosystem for scalable data sharing in cloud storage. IEEE Trans. Parallel Distrib. Syst., 25(2):468–477, 2014.

[13] C.-K. Chu and W.-G. Tzeng. Identity-based proxy re-encryption without random oracles. In J. A. Garay, A. K.

Lenstra, M. Mambo, and R. Peralta, editors, ISC, volume 4779 of LNCS, pages 189–202. Springer, 2007.

[14] R. Cramer and V. Shoup. Design and analysis of practical publickey encryption schemes secure against adaptive chosen ciphertext attack. SIAM J. Comput., 33(1):167–226, January 2004.

[15] Y. Dodis, Y. T. Kalai, and S. Lovett. On cryptography with auxiliary input. In STOC, pages 621–630. ACM, 2009.

[16] Y. Dodis, J. Katz, S. Xu, and M. Yung. Key-insulated public key cryptosystems. In EUROCRYPT, volume 2332 of Lecture Notes in Computer Science, pages 65–82. Springer, 2002.

[17] Y. Dodis, J. Katz, S. Xu, and M. Yung. Strong key-insulated signature schemes. In Public Key Cryptography, volume 2567 of Lecture Notes in Computer Science, pages 130–144. Springer, 2003.

[18] L. Ferretti, M. Colajanni, and M. Marchetti. Distributed, concurrent, and independent access to encrypted cloud databases. IEEE Trans. Parallel Distrib. Syst., 25(2):437–446, 2014.

[19] C. Gentry. Certificate-based encryption and the certificate revocation problem. In EUROCRYPT, volume 2656 of Lecture Notes in Computer Science, pages 272–293. Springer, 2003.

[20] M. Green and G. Ateniese. Identity-based proxy re-encryption. In ACNS '07, volume 4512 of LNCS, pages 288–306. Springer, 2007.

[21] H. Guo, Z. Zhang, J. Zhang, and C. Chen. Towards a secure certificateless proxy re-encryption scheme. In W. Susilo and R. Reyhanitabar, editors, ProvSec, volume 8209 of Lecture Notes in Computer Science, pages 330–346. Springer, 2013.

[22] G. Hanaoka, Y. Hanaoka, and H. Imai. Parallel key-insulated public key encryption. In Public Key Cryptography, volume 3958 of Lecture Notes in Computer Science, pages 105–122. Springer, 2006.

[23] Y. H. Hwang, J. K. Liu, and S. S. M. Chow. Certificateless public key encryption secure against malicious kgc attacks in the standard model. J. UCS, 14(3):463–480, 2008.

[24] 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.

[25] B. Libert, J.-J. Quisquater, and M. Yung. Parallel key-insulated public key encryption without random oracles. In Public Key Cryptography, volume 4450 of Lecture Notes in Computer Science, pages 298–314. Springer, 2007.

Valluri Venkatalakshmi is a student of Sri Sunflower college of engineering college,Lankapalli.she is studying M.tech[CSE] and also received B.tech degree from JNTUK University

Jetti Sri lakshmi is a Assistant professor in Sri Sunflower college of engineering and technology ,Lankapalli she received Master Degree from different colleges.Having 2+ years of Experience as a faculty and Guide for Different Domains.