INTERNATIONAL JOURNAL · ENGINEERING RESEARCH ·

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

COPY RIGHT

NON SOLUS

ELSEVIER

SSRN

IJIEMR Transactions, online available on 15th Nov 2018. Link :http://www.ijiemr.org/downloads.php?vol=Volume-07&issue=ISSUE-12

Title: A NOVEL APPROACH FOR PRIVACY AND ENCRYPTED DATA SEARCH IN CLOUD SERVICE

Volume 07, Issue 12, Pages: 195–199.

Paper Authors

VALIVETI DEVI VARA PRASAD, MD.IMRAN

Nimra College of Engineering & Technology, A.P., India.

International Journal for Innovative Engineering and Management Research ★

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

A NOVEL APPROACH FOR PRIVACY AND ENCRYPTED DATA SEARCH IN CLOUD SERVICE

[1]VALIVETI DEVI VARA PRASAD, [2]MD.IMRAN

[1]Student, M. Tech (CSE), NIMRA INSTITUTE OF SCIENCE & TECHNOLOGY, A.P., India.

[2]Assistant Professor, Dept. of Computer Science & Engineering, NIMRA INSTITUTE OF SCIENCE & TECHNOLOGY, A.P., India.

[1]devi-dvpvaliveti@gmail.com

Abstract — In other words Cloud Computing is the use of computing resources that are delivered as a service over a network." So, you push your data to the cloud then tell the cloud what computation to perform. The cloud computes the result and sends the answer back to you. Hence the data can be accessed from any remote location via internet. However doing so may give rise to certain privacy implications. As Cloud is not trusted. In this paper, Document storage in the cloud infrastructure is rapidly gaining popularity throughout the world. However, it poses risk to consumers unless the data is encrypted for security. Encrypted data should be effectively searchable and retrievable without any privacy leaks, particularly for the mobile client. Although recent research has solved many security issues, the architecture cannot be applied on mobile devices directly under the mobile cloud environment. This is due to the challenges imposed by wireless networks, such as latency sensitivity, poor connectivity, and low transmission rates. This leads to a long search time and extra network traffic costs when using traditional search schemes. This study addresses these issues by proposing an efficient Encrypted Data Search scheme as a mobile cloud service.

Keywords — Encryption, Cloud, security

INTRODUCTION

Now a day's large amount of data accumulated on cloud. All information stored on cloud throughout the world. It will be unsecure unless all data encoded for the security purpose. Crumbled information arranges properly to be effectively and easily for searchable and retrievable data with no security access, especially for the versatile customer. Number of issue find out in previous studies relates to cloud data. Especially in portable cloud platform cell phone can't be connected it may cause to difficulties occurred remote systems. For example, inertness affectability, poor availability, and low transmission rates. To protect data security, the documents and their indexes are usually encrypted before outsourcing to the cloud for searches. When users need to query certain documents, they first send keywords to the original data provider. The provider then generates encrypted keywords (also called trapdoors) and returns the trapdoors to the user. The user then sends these trapdoors to the cloud.

Upon receiving the trapdoors, the Cloud uses a special search algorithm to select a set of desired documents (encrypted) based on the encrypted indexes and given trapdoors. Finally, the user receives these encrypted search results and uses the private key from the provider to decrypt documents. This architecture, as depicted in this system, protects data security while entitling the providers to use both the computation and storage power of the Cloud for document searches. Due to these advantages, this architecture has already been well-adopted in privacy preserving search systems Mobile devices (e.g. smart phones and tablets) were estimated to surpass two billion growth (0.3 billion for PCs) in the year 2014, which dominates the overall shipment of consumer electronics devices. Nowadays, users heavily utilize mobile devices to request document search services. In general, mobile devices connect to the Internet mainly via wireless networks (Wi-Fi/3G/4G/LTE), which incurs some challenges as compared to traditional wired networks. These challenges include:

1) Latency sensitivity: these wireless networks incur longer network latency, which can slow down a single search request if the search request requires many network round trips. For example, in the traditional design shown in Figure 1, a single search requires three round trips and results in notable latency for wireless communication.

2) Poor connectivity: Mobile devices are normally incapable of maintaining a long-running connection with the Cloud, mostly for energy-saving purposes. Multiple search requests could incur numerous re-connection operations and extra authentication costs.

3) Low network transmission rate: Mobile devices are normally equipped with low-power transmission components, bringing slower transmission rates.

PROPOSED SYSTEM

The ranked keyword search will return documents to the relevance score. Zero et al. proposed a novel technique that makes the server side carry out the search operation. However, it should send many unrelated documents back and let the user filter them. This is a waste of traffic, which is unsuitable for the mobile cloud. Bowers et al.proposed a distributed cryptographic system that preserved the security of the document retrieval process and the high availability of The system, but this system suffers from two network round trips and calculation complexity for target documents. Wang et al. proposed a single round trip encrypted search scheme, but their system is not secure enough, as it leaks the keyword and associated document information from multiple keyword searches. Li et al. proposed a single-keyword encryption search scheme utilizing ranked keyword search, which network communication between the user and the cloud by transferring the computing burden from the user to the cloud.

Advantages:

- We proposed a novel encrypted search system EnDAS over the mobile cloud, which improves network traffic and search time efficiency compared with the traditional system.

- We started with a thorough analysis of the traditional encrypted search system and. analysed its bottlenecks in the mobile cloud: network traffic and search time inefficiency. Then we developed an efficient architecture of EnDAS which is suitable for the mobile cloud to address these issues, where we utilized the TMT module.
- RSBS algorithm to cope with the inefficient search time issue, while a trapdoor compression method was employed to reduce network traffic costs. Finally our evaluation study experimentally demonstrates the performance advantages of EnDAS

LITERATURE SURVEY

Secure kNN computation on encrypted databases

AUTHORS: W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis

Service providers like Google and Amazon are moving into the SaaS (Software as a Service) business. They turn their huge infrastructure into a cloud-computing environment and aggressively recruit businesses to run applications on their platforms. To enforce security and privacy on such a service model, we need to protect the data running on the platform. Unfortunately, traditional encryption methods that aim at providing "unbreakable" protection are often not adequate because they do not support the execution of applications such as database queries on the encrypted data. In this paper we discuss the general problem of secure computation on an encrypted database and propose a SCONEDB Secure Computation ON an Encrypted Database) model, which captures the execution and security requirements. As a case study, we focus on the problem of k-nearest neighbour (kNN) computation on an encrypted database. We develop a new asymmetric scalar-product-preserving encryption (ASPE) that preserves a special type of scalar product. We use APSE to construct two secure schemes that support kNN computation on encrypted data; each of these schemes is shown to resist practical attacks of a different background knowledge level, at a different overhead cost. Extensive performance studies are carried out to evaluate the overhead and the efficiency of the schemes.

RELATED WORK

For data security, the previous encryption algorithms cannot directly apply to mobile cloud, because it is hard to achieve efficient network traffic and search time to address the important issues for mobile cloud. Agrawal et al. [21] proposed a one-to-one mapping order preserving encryption method; however, it leads to information leaks. Wang et al. [3] proposed a one-to-many mapping order preserving encryption method that requires a complex computation process, and therefore is not suitable for the mobile cloud. Wang et al. [4] and Swami Nathan et al. [22] employed an order-preserving encryption [23] method to retrieve data from encrypted cloud data, which preserved security perfectly. However, this can only be applied in a single-keyword search that retrieves files in a coarse granularity. Some researchers solved this problem through fully homomorphic encryption [5], [24], [25], [26], to retain the security of the encrypted search scheme. In a word, these Order Preserving Encryption (OPE) algorithms [23], [21] and fully homomorphic encryption [5], [24], [25], [26] methods proved themselves secure and accurate enough for searching encrypted data purpose. However, they cost many computing resources. As network traffic and search time efficiency becoming important, a complicated algorithm is not suitable in mobile devices. So we choose an efficient encryption algorithm, fast accumulated hash (FAH) [11], [12], [13], to encrypt document's index and keywords in EnDAS.

1. Encryption: In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text (ibid.). This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message.

2. Decryption: An authorized party, however, is able to decode the cipher text using a decryption algorithm that usually requires a secret decryption key that adversaries do not have access to. For technical reasons, an encryption scheme usually needs a key-generation algorithm, to randomly produce keys

RSS ALGORITHM: RANKED SERIAL SEARCH.

Cryptographic: (a process called encryption), Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

- Plaintext:

Most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text)

- Cliphertext:

Cipher text is then back again (known as decryption). Individuals who practice this field are known as cryptographers.

CONCLUSION

In this paper, proposed a novel encrypted search system EnDAS over the mobile cloud, which improves network traffic and search time efficiency compared with the traditional system. We started with a thorough analysis of the traditional encrypted search system and analysed its bottlenecks in the mobile cloud: network traffic and search time inefficiency. Then we developed an efficient architecture of EnDAS which is suitable for the mobile cloud to address these issues, where we utilized the TMT module and the RSBS algorithm to cope with the inefficient search time issue, while a trapdoor compression method was employed to reduce network traffic costs. Finally our evaluation study experimentally demonstrates the performance advantages of EnDAS.

References

[1] D. Huang, "Mobile cloud computing," IEEE COMSOC Multimedia Commun. Tech. Committee (MMTC) E-Letter, vol. 6, no. 10, pp. 27– 31, 2011.

[2] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword

ranked search over encrypted cloud data," in Proc. Int. Conf. Comput. Commun. (INFOCOM), Apr. 2011, pp. 829–837.

[3] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," IEEE Trans. Parallel Distrib. Systems, vol. 23, no. 8, pp. 1467–1479, 2012.

[4] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS), Jun. 2010, pp. 253–262.

[5] C. Gentry and S. Halevi, "Implementing gentrys fullyhomomorphic encryption scheme," in Advances in Cryptology– EUROCRYPT 2011, 2011, pp. 129–148.

[6] C. O¨ rencik and E. Savas¸, "Efficient and secure ranked multikeyword search on encrypted cloud data," in Proc. Joint EDBT/ICDT Workshops, Mar. 2012, pp. 186–195.

[7] Gartner, "Worldwide traditional pc, tablet, ultramobile and mobile phone shipments on pace to grow 7.6 percent in 2014,"http://www.gartner.com/newsroom/id/2645115.

[8] Trellian, "Keywords number," http://www.keyworddiscovery.com/keyword-stats.html? Date=2014-03-01.

[9] V. Rijmen and J. Daemen, "Advanced encryption standard," Federal Information Processing Standard, pp. 19–22, 2001.

[10] X. Lai, "On the design and security of block ciphers," Ph.D. dissertation, Diss. Techn. Wiss ETH Z¨ urich, Nr. 9752, 1992. Ref.: JL Massey; Korref.: H. B¨ uhlmann, 1992.

[11] K. Nyberg, "Fast accumulated hashing," in Proc. Int. Workshop Fast Softw. Encryption (FSE), Feb. 1996, pp. 83–87.

[12] Nyberg and Kaisa, "Commutativity in cryptography," in Proc. Int. Workshop Funct. Anal., 1995.

[13] J. Benaloh and M. De Mare, "One-way accumulators: A decentralized alternative to digital signatures," in Advances in Cryptology- EUROCRYPT 1993, 1994, pp. 274–285.

[14] C. O¨ rencik and E. Savas¸, "An efficient privacy-preserving multikeyword search over encrypted cloud data with ranking," Distrib. Parallel Databases, vol. 32, no. 1, pp. 119–160, Mar. 2014.

[15] P. Wang, H. Wang, and J. Pieprzyk, "An efficient scheme of common secure indices for conjunctive keyword-based retrieval on encrypted data," pp. 145–159, 2009.