An EFficiency and Privacy-Preserving Biometric Identification Scheme in Cloud Computing

Gireesh Chebrolu, Sai Dinesh, Dhipauk Joqim

Under the guidance of Sri jayanthi.S, Assistant Professor
Department of Computer Science and Engineering
RMK Engineering College, Tamil Nadu, India

---***---

Abstract – Outsourcing of data into cloud has become an effective trend in modern day computing due to its ability to provide low-cost, pay-as-you-go IT services. Although cloud based services offer many advantages, privacy of the outsourced data is a big concern. To mitigate this concern, it is desirable to outsource sensitive data in an encrypted form but cost of encryption process would increase the heavy computational overhead on thin clients such as resource-constrained mobile devices. Recently, several keyword searchable encryption schemes have been described in the literature. However, these schemes are not effective for resource-constrainedmobile devices, because the adopted encryption system should not only support keyword search over the encrypted data but also offer high performance. In this paper, we propose an efficient and secure privacy-preserving approach for outsourced data of resource-constrained mobile devices in the cloud computing. Our approach employs probabilistic public key encryption algorithm for encrypting the data and invoke ranked keyword search over the encrypted data to retrieve the files from the cloud. We aim to achieve an efficient system for data encryption without sacrificing the privacy of data. Further, our ranked keyword search greatly improves the system usability by enabling ranking based on relevance score for search result, sends top most relevant files instead of sending all files back, and ensures the file retrieval accuracy. As a result, data privacy ensures computation, communication overheads in reduction. Thorough security and performance analysis, we prove that our approach is semantically secure and efficient.

1. INTRODUCTION

Besides, all of these advantages of outsourced data in Cloud, there are also some significant issues. One of the major issues is the privacy of outsourced data in cloud (Jaeger and Schiffman, 2010) i.e., the sensitive information such as e-mail, health records, and government data may leak to unauthorized users (Slocum, 2009; Krebs, 2009) or even be hacked (Cloud Security Alliance, 2009). Since, the cloud is an open platform; it can be subjected to attacks from both malicious insiders and outsiders (Haclgiimfi et al., 2002). The Cloud service providers (CSPs) usually provide data security through mechanisms like firewalls and virtualization. However, these mechanisms do not protect users' privacy from the CSP itself due to remote cloud storage servers are untrusted. A natural approach to preserve the privacy of sensitive data is to encrypt data before outsourcing it into the cloud and retrieves the data back through keyword based search over encrypted data. Although encryption provides protection from illegal accesses, it significantly increases the computation overhead on the data owners especially when they having resource-constrained mobile devices and large size of data files.

2. LITERATURE REVIEW

2.1.1 A Berkeley view of cloud computing

Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS), so we use that term. The datacenter hardware and software is what we will call a Cloud. When a Cloud is made available in a pay-as-you-go manner to the public, we call it a Public Cloud; the service being sold is Utility Computing. Current examples of public Utility Computing include Amazon Web Services, Google AppEngine, and Microsoft Azure. We use the term Private Cloud to refer to internal datacenters of a business or other organization that are not made available to the public. Thus, Cloud Computing is the sum of SaaS and Utility Computing, but does not normally include Private Clouds. We'll generally use Cloud Computing, replacing it with one of the other terms only when clarity demands it. Figure 1 shows the roles of the people as users or providers of these layers of Cloud Computing, and we'll use those terms to help make our arguments clear.

The advantages of SaaS to both end users and service providers are well understood. Service providers enjoy greatly simplified software installation and maintenance and centralized control over versioning; end users can access the service "anytime, anywhere", share data and collaborate more easily, and keep their data stored safely in the infrastructure.

2.1.2 Private Query on Encrypt Data in Multi-User Settings

Searchable encryption schemes allow users to perform keyword based searches on an encrypted database. Almost all existing such schemes only consider the scenario where a single user acts as both the data owner and the querier. However, most databases in practice do not just serve one user; instead, they support search and write operations by multiple users. In this paper, we systematically study searchable encryption in a practical multi-user setting. Our results include a set of security notions for multi-user searchable encryption as well as a construction which is provably secure under the newly introduced security notions

2.1.3 Efficient Public Key Encryption with Disjunctive Keywords Search Using the New Keywords

Public key encryption with disjunctive keyword search (PEDK) is a public key encryption scheme that allows disjunctive keyword search over encrypted data without decryption. This kind of scheme is crucial to cloud storage and has received a lot of attention in recent years. However, the efficiency of the previous scheme is limited due to the selection of a less efficient converting method which is used to change query and index keywords into a vector space model. To address this issue, we design a novel converting approach with better performance, and give two adaptively secure PEDK schemes based on this method. The first one is built on an efficient inner product encryption scheme with less searching time, and the second one is constructed over composite order bilinear groups with higher efficiency on index and trapdoor construction. The theoretical analysis and experiment results verify that our schemes are more efficient in time and space complexity as well as more suitable for the mobile cloud setting compared with the state-of-art schemes.

2.2.1 EXISTING SYSTEM

For predicates corresponding to the evaluation of inner products over ZN (for some large integer N). This, in turn, enables constructions in which predicates correspond to the evaluation of disjunctions, polynomials, CNF/DNF formulae, or threshold predicates (among others). Besides serving as a significant step forward in the theory of predicate encryption, our results lead to a number of applications that are interesting in their own right. Predicate encryption is a new paradigm for public-key encryption generalizing, among other things, identity-based encryption. In a predicate encryption scheme, secret keys correspond to predicates and ciphertexts are associated with attributes; the secret key SKf corresponding to a predicate f can be used to decrypt a ciphertext associated with attribute I if and only if f(I) = 1. Constructions of such schemes are currently known for certain classes of predicates. We construct such a scheme

3.1 PROPOSED SYSTEM

We consider the following problem: a user $\mathcal{U}$ wants to store his files in an encrypted form on a remote fil server $\mathcal{S}$. Later the user $\mathcal{U}$ wants to efficiently retrieve some of the encrypted files containing (or indexed by) specific keywords, keeping the keywords themselves secret and not jeopardizing the security of the remotely stored files. For example, a user may want to store old e-mail messages encrypted on a server managed by Yahoo or another large vendor, and later retrieve certain messages while travelling with a mobile device. In this paper, we offer solutions for this problem under well-defined security requirements. Our schemes are efficient in the sense that no public-key cryptosystem is involved. Indeed, our approach is independent of the encryption method chosen for the remote files. They are also incremental, in that $\mathcal{U}$ can submit new files which are secure against previous queries but still searchable against future queries.

3.3 SYSTEM ARCHITECTURE

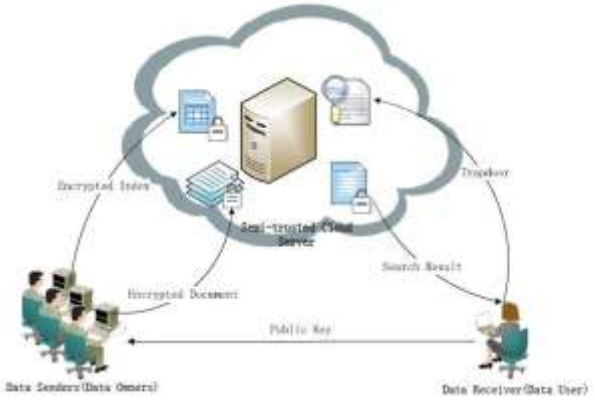
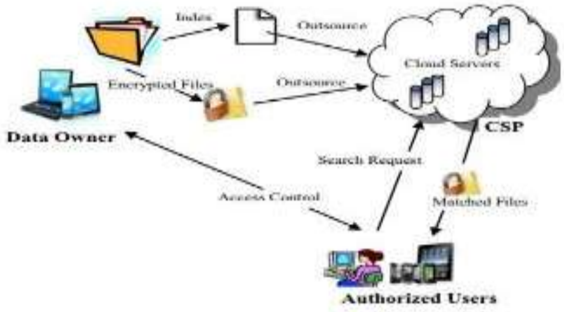


Fig 3.3: Architecture diagram

3.4 SYSTEM DESIGN



REFERNCES

1. Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, A. Konwinski A, Lee G, Patterson DA, Rabkin A, Stoica I, Zaharia M. Above the clouds: a Berkeley view of cloud computing, Technical Report UCB-EECS-2009-28. Berkeley: University of California; 2009. p. 1–23

2. Attrapadung N, Li Bert B. Functional encryption for inner product: achieving constant size cipher text switch adaptive security or support for negation. In: Nguyen P, Pointcheval D, editors. Public Key Cryptography, 6056 LNCS. Springer Berlin/Heidelberg; 2010. p. 384–402.

3. Bao F, Deng R, Ding X, Yang Y. Private query on encrypted data in multi-user settings. In: Proceedings of 4th international conference on information security practice and experience. Sydney; 2008. p. 71–85

4. Bellare M, Boldyreva A, Neill AO. Deterministic and efficient searchable encryption. In: Menezes A, editor. Advances in Cryptology-CRYPTO 2007, 4622 LNCS. Berlin/ Heidelberg: Springer; 2007. p. 535–52.

5. Boldyreva A, Chenette N, Lee Y, O'Neill A. Order-preserving symmetric encryption. In: Proceedings of 28th annual international conference on theory and applications of cryptography techniques. Springer, Germany; 2009. p. 224–41.

6. Boneh D, Crescenzo GD, Ostrovsky R, Persiano G. Public key encryption with keyword search. In Proceedings of international conference on theory and applications of cryptographic techniques: advances in cryptology. Switzerland; 2004. p. 506–22.

7. Cao N, Wang C, Li M, Ren K, Lou W. Privacy-preserving multi-keyword ranked search over encrypted cloud data. IEEE Trans Parallel Distrib Syst 2014;25 (1):222–33

8. Chang Y-C, Mitzenmacher M. Privacy preserving keyword searches on remote encrypted data. In: Proceeding of Third International Conference on Applied Cryptography and Network Security. New York; 2005. p. 442–55.

9. Curtmola R, Garay JA, Kamara S, Ostrovsky R. Searchable symmetric encryption: improved definitions and efficient constructions. In: Proceedings of 13th ACM conference on computer and communication security. Alexandaria; 2006. p. 79–88

10. RFC: Request for comments database; 2012 ⟨http://www.ietf.org/rfc.html⟩. Shi E, Bethencourt J, Chan H, Song D, Perrig A. Multi-dimensional range query over encrypted data. In: Proceedings of IEEE symposium on security and privacy. California; 2007. p. 350–64.

11. Slocum Z. Your Google docs: soon in search results?; 2009. ⟨http://news.cnet.com/ 8301-17939_109-10357137-2.html⟩.

12. Song D, Wagner D, Perrig A. Practical techniques for searches on encrypted data. In: Proceedings of the IEEE symposium on security and privacy. California; 2000. p. 44–55.

13. Wang C, Cao N, Ren K, Lou W. Enabling secure and efficient ranked keyword search over outsourced cloud data. IEEE Trans Parallel Distrib Syst 2012;23 (8):1467–79.

14.Waters B, Balfanz D, Durfee G, Smetters D. Building an encrypted and searchable audit log. In: Proceedings of annual network and distributed security symposium. California; 2004.

15. Witten IH, Moffat A, Bell TC. Managing gig a bytes: compressing and indexing documents and images. Second ed. CA, USA: Morgan Kaufmann Series; 1999. Yu J, Lu P, Zhu Y, Xue G, Li M. Toward secure multi-keyword top-k retrieval over encrypted cloud data. IEEE Trans Depend Secur Comput 2013;10(4):239–50