Dual-Server Public-key Encryption with Keyword Search for Secure Cloud Storage

A.VIJAYA DURGA [1], N. KOTESWARAMMA [2], B. LAKSHMI PRAVEENA [3]
[1,2]*Dept. of MCA, VVIT, Guntur, AP*
[3]*Dept. of IT, VVIT, Guntur, AP*

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, we propose a new PEKS framework named dual-server PEKS (DS-PEKS). As another main contribution, we define a new variant of the smooth projective hash functions (SPHFs) referred to as linear and homomorphic SPHF (LH-SPHF). We then show a generic construction of secure DS-PEKS from LH-SPHF. To illustrate the feasibility of our new framework, we provide an efficient instantiation of the general framework from a Decision Diffie–Hellman-based LH-SPHF and show that it can achieve the strong security against inside the KGA.

Indexed Terms -- Location-based social network, text mining, travel route recommendation.

I. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers. Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. The model is shown in figure below. If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider.

Benefits of cloud computing:

1. Achieve economies of scale – increase volume output or productivity with fewer people. Your cost per unit, project or product plummets.
2. Reduce spending on technology infrastructure. Maintain easy access to your information with minimal upfront spending. Pay as you go (weekly, quarterly or yearly), based on demand.
3. Globalize your workforce on the cheap. People worldwide can access the cloud, provided they have an Internet connection.
4. Streamline processes. Get more work done in less time with less people.
5. Reduce capital costs. There's no need to spend big money on hardware, software or licensing fees.
6. Improve accessibility. You have access anytime, anywhere, making your life so much easier!
7. Monitor projects more effectively. Stay within budget and ahead of completion cycle times.
8. Less personnel training is needed. It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues.
9. Minimize licensing new software. Stretch and grow without the need to buy expensive software licenses or programs.
10. Improve flexibility. You can change direction without serious "people" or "financial" issues at stake.

II. EXISTING SYSTEM

In a PEKS system, using the receiver's public key, the sender attaches some encrypted keywords (referred to as PEKS ciphertexts) with the encrypted data. The receiver then sends the trapdoor of a to-be-searched keyword to the server for data searching. Given the trapdoor and the PEKS ciphertext, the server can test whether the keyword underlying the PEKS ciphertxt is equal to the one selected by the receiver. If so, the server sends the matching encrypted data to the receiver.

Baek *et al.* proposed a new PEKS scheme without requiring a secure channel, which is referred to as a secure channel-free PEKS (SCF-PEKS).

III. PROPOSED SYSTEM

The contributions of this paper are four-fold.

We formalize a new PEKS framework named *Dual-Server Public Key Encryption with Keyword Search* (DS-PEKS) to address the security vulnerability of PEKS.

A new variant of *Smooth Projective Hash Function* (SPHF), referred to as *linear and homomorphic SPHF*, is introduced for a generic construction of DS-PEKS.

We show a generic construction of DS-PEKS using the proposed Lin-Hom SPHF.

To illustrate the feasibility of our new framework, an efficient instantiation of our SPHF based on the Diffie-Hellman language is presented in this paper.

1. Proposed Algorithm:

A DS-PEKS scheme is defined by the following algorithms

- Setup(y): Takes as input the security parameter _y, generates the system parameters P.
- KeyGen(P): Takes as input the systems parameters P,outputs the public/secret key pairs (pkFS; skFS), and (pkBS; skBS) for the front server, and the back server respectively.
- DS-PEKS (P; pkFS; pkBS; kw1): Takes as input P, the front server's public key pkFS, the back server's public key pkBS and the keyword kw1, outputs the PEKS ciphertext CTkw1 of kw1.
- DS-Trapdoor (P; pkFS; pkBS; kw2): Takes as input P, the front server's public key pkFS, the back server's public key pkBS and the keyword kw2, outputs the trapdoorTkw2.
- BackTest(P; skBS;CITS): Takes as input P, the back server's secret key skBS and the internal testing-state CITS, outputs the testing result 0 or 1.

2. Implementation of Modules:

Modules:

- System Construction Module
- Semantic-Security against Chosen Keyword Attack
- Front Server
- Back Server

Modules Description:

- System Construction Module:

In the first module, we develop the system with the entities required to provde our system. 1) Cloud User: the user, who can be an individual or an organization originally storing their data in cloud and accessing the data. 2) Cloud Service Provider (CSP): the CSP, who manages cloud servers (CSs) and provides a paid storage space on its infrastructure to users as a service. We propose a new framework, namely DS-PEKS, and present its formal definition and security models. We then define a new variant of smooth projective hash function (SPHF). A generic construction of DS-PEKS from LH-SPHF is shown with formal correctness analysis and security proofs. Finally, we present an efficient instantiation of DS-PEKS from SPHF.

- Semantic-Security against Chosen Keyword Attack:

In the module, we develop the semantic-security against chosen keyword attack which guarantees that no adversary is able to distinguish a keyword from another one given the corresponding PEKS cipher text. That is, the PEKS cipher text does not reveal any

information about the underlying keyword to any adversary.

- Front Server:

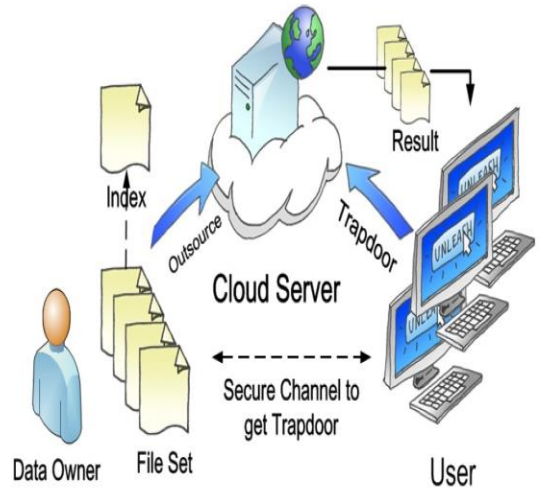
After receiving the query from the receiver, the front server pre-processes the trapdoor and all the PEKS ciphertexts using its private key, and then sends some internal testing-states to the back server with the corresponding trapdoor and PEKS ciphertexts hidden.

- Back Server:

In this module, the back server can then decide which documents are queried by the receiver using its private key and the received internal testing-states from the front server.

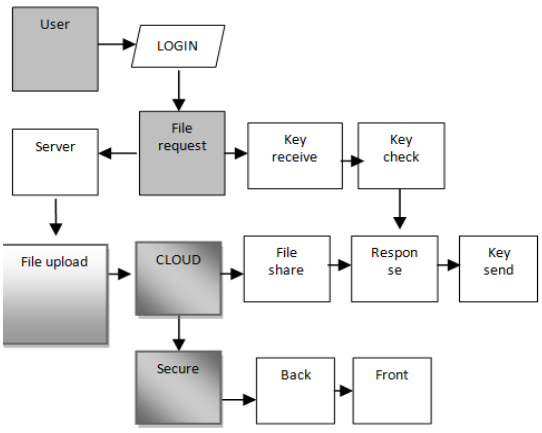
3. System Architectural Design

Architecture Diagram:



User Interface:

Data Flow Diagram:



IV. RELATED WORK

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams.

1. Tools and Technologies used:

In this project I used:

a) Java Technology:

Java technology is both a programming language and a platform.

b) The Java Programming Language

The Java programming language is a high-level language

c) SQL Management Server 2014 technologies

2. Literature Survey:

a) A new general framework for secure public key encryption with keyword search

AUTHORS: R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang

Public Key Encryption with Keyword Search (PEKS), introduced by Boneh et al. in Eurocrypt'04, allows users to search encrypted documents on an untrusted server without revealing any information. This notion is very useful in many applications and has attracted a lot of attention by the cryptographic research community. However, one limitation of all the existing PEKS schemes is that they cannot resist the Keyword Guessing Attack (KGA) launched by a malicious server. In this paper, we propose a new PEKS framework named Dual-Server Public Key Encryption with Keyword Search (DS-PEKS). This new framework can withstand all the attacks, including the KGA from the two untrusted servers, as long as they do not collude. We then present a generic construction of DS-PEKS using a new variant of the Smooth Projective Hash Functions (SPHFs), which is of independent interest.

b) Searchable symmetric encryption: Improved definitions and efficient constructions

AUTHORS: R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky

Searchable symmetric encryption (SSE) allows a party to outsource the storage of his data to another party in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research and several security definitions and constructions have been proposed. In this paper we begin by reviewing existing notions of security and propose new and stronger security definitions. We then present two constructions that we show secure under our new definitions. Interestingly, in addition to satisfying stronger security guarantees, our constructions are more efficient than all previous constructions.

Further, prior work on SSE only considered the setting where only the owner of the data is capable of submitting search queries. We consider the natural extension where an arbitrary group of parties other than the owner can submit search queries. We formally define SSE in this multi-user setting, and present an efficient construction.

c) Public Key Encryption with Keyword Search based on K-Resilient IBE

AUTHORS: D. Khader

Abstract. An encrypted email is sent from Bob to Alice. A gateway wants to check whether a certain keyword exists in an email or not for some reason (e.g. routing). Nevertheless Alice does not want the email to be decrypted by anyone except her including the gateway itself. This is a scenario where public key encryption with keyword search (PEKS) is needed. In this paper we construct a new scheme (KR-PEKS) the KResilient Public Key Encryption with Keyword Search. The new scheme is secure under a chosen keyword attack without the random oracle. The ability of constructing a Public Key Encryption with Keyword Search from an Identity Based Encryption was used in the construction of the KR-PEKS. The security of the new scheme was proved by showing that the used IBE has a notion of key privacy. The scheme was then modified in two different ways in order to fulfill each of the following: the first modification was done to enable multiple keyword searches and the other was done to remove the need of secure channels.

d) Generic constructions of secure-channel free searchable encryption with adaptive security

AUTHORS: K. Emura, A. Miyaji, M. S. Rahman, and K. Omote

For searching keywords against encrypted data, public key encryption scheme with keyword search (PEKS), and its extension secure-channel free PEKS (SCF-PEKS), has been proposed. In this paper, we extend the security of SCF-PEKS, calling it adaptive SCF-PEKS, wherein an adversary (modeled as a "malicious-but-legitimate" receiver) is allowed to issue test queries adaptively. We show that adaptive SCF-PEKS can be generically constructed by anonymous identity-based encryption only. That is, SCF-PEKS can be constructed without any additional cryptographic primitive when compared with the Abdalla et al. PEKS construction (J. Cryptology 2008), even though adaptive SCF-PEKS requires additional functionalities. We also propose other adaptive SCF-PEKS construction, which is not fully generic but is efficient compared with the first one. Finally, we instantiate an adaptive SCF-PEKS scheme (via our second construction) that achieves a similar level of efficiency for the costs of the test procedure and encryption, compared with the (non-adaptive secure) SCF-PEKS scheme by Fang et al. (CANS2009). Copyright © 2014 John Wiley & Sons, Ltd. 5) Cooperative provable data possession for integrity verification in multicloud storage

e) Off-line keyword guessing attacks on recent public key encryption with keyword search schemes

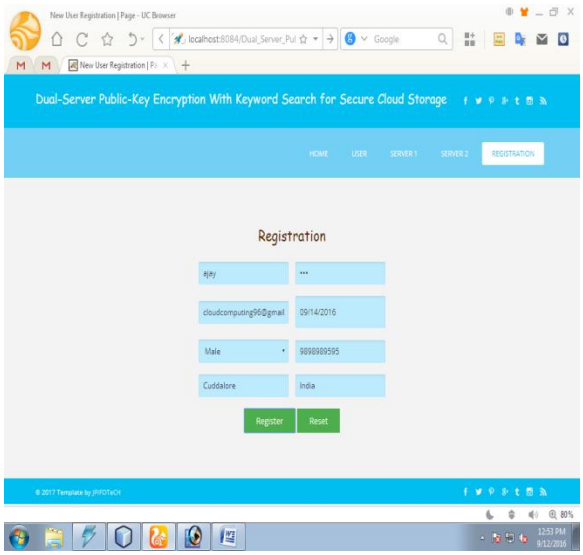
AUTHORS: W.-C. Yau, S.-H. Heng, and B.-M. Goi

The Public Key Encryption with Keyword Search Scheme (PEKS) was first proposed by Boneh et al. in 2004. This scheme solves the problem of searching on data that is encrypted using a public key setting. Recently, Baek et al. proposed a Secure Channel Free Public Key Encryption with Keyword Search (SCF-PEKS) scheme that removes the secure channel for sending trapdoors. They later proposed another improved PEKS scheme that integrates with a public key encryption (PKE) scheme, called PKE/PEKS. In this paper, we present off-line keyword guessing attacks on SCF-PEKS and PKE/PEKS schemes. We demonstrate that outsider adversaries that capture the trapdoors sent in a public channel can reveal encrypted keywords by performing off-line keyword guessing

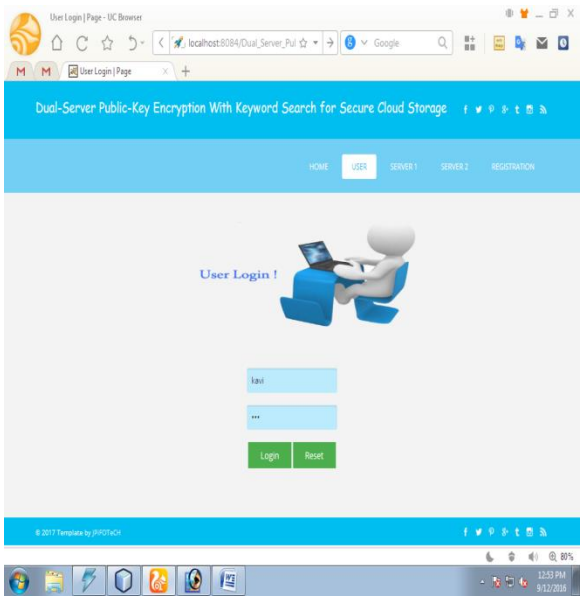
attacks. While, insider adversaries can perform the attacks regardless the trapdoors sent in a public or secure channel.

3. Result:

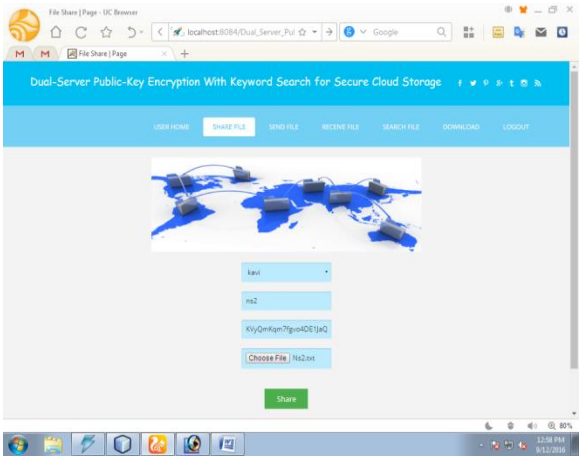
a) User Registration:



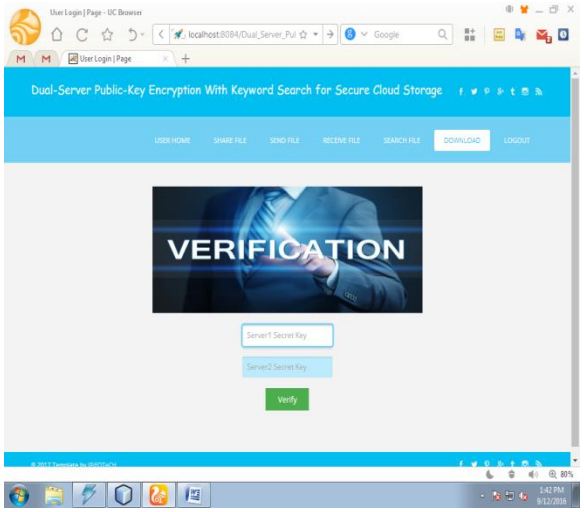
b) User Login:



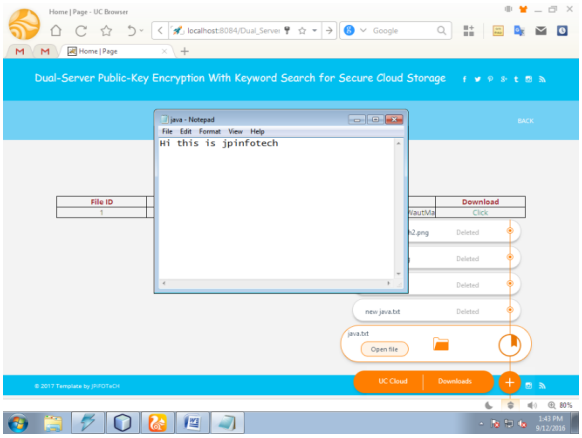
c) Share File:



d) Verification:



e) File Upload:



V. CONCLUSION AND FUTURE SCOPE

In this paper, we proposed a new framework, named Dual-Server Public Key Encryption with Keyword Search (DS-PEKS), that can prevent the inside keyword guessing attack which is an inherent vulnerability of the traditional PEKS framework. We also introduced a new Smooth Projective Hash Function (SPHF) and used it to construct a generic DS-PEKS scheme. An efficient instantiation of the new SPHF based on the Diffie-Hellman problem is also presented in the paper, which gives an efficient DS-PEKS scheme without pairings.

VI. ACKNOWLEDGEMENT

I convey my thanks to my HOD
Smt. Dr. N. KOTESWARAMMA for providing me with help and support.

I convey my sincere thanks to my guide
Smt. B. LAKSHMI PRAVEENA for providing me support and details at the right time and during the progressive reviews.

My gratitude is extended to the department staff and technicians for prompt help when required.

This project is dedicated to my classmates and my parents.

REFERENCES

[1] R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, "A new general framework for secure public key encryption with keyword search," in *Proc. 20th Australasian Conf. Inf. Secur. Privacy (ACISP)*, 2015, pp. 59–76.

[2] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. IEEE Symp. Secur. Privacy*, May 2000, pp. 44–55.

[3] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in *Proc. ACM SIGMOD Int. Conf. Manage. Data*, 2004, pp. 563–574.

[4] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in *Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS)*, 2006, pp. 79–88.

[5] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Proc. Int. Conf. EUROCRYPT*, 2004, pp. 506–522.

[6] R. Gennaro and Y. Lindell, "A framework for password-based authenticated key exchange," in *Proc. Int. Conf. EUROCRYPT*, 2003, pp. 524–543.

[7] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "Building an encrypted and searchable audit log," in *Proc. NDSS*, 2004, pp. 1–11.

[8] M. Abdalla *et al.*, "Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions," in *Proc. 25th Annu. Int. Conf. CRYPTO*, 2005, pp. 205–222.

[9] D. Khader, "Public key encryption with keyword search based on K-resilient IBE," in *Proc. Int. Conf. Comput. Sci. Appl. (ICCSA)*, 2006, pp. 298–308.

[10] P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack," *IEEE Trans. Comput.*, vol. 62, no. 11, pp. 2266–2277, Nov. 2013.

[11] G. Di Crescenzo and V. Saraswat, "Public key encryption with searchable keywords based on Jacobi symbols," in *Proc. 8th Int. Conf. INDOCRYPT*, 2007, pp. 282–296.

[12] C. Cocks, "An identity based encryption scheme based on quadratic residues," in *Cryptography and Coding*. Cirencester, U.K.: Springer, 2001, pp. 360–363.

[13] J. Baek, R. Safavi-Naini, and W. Susilo, "Public key encryption with keyword search revisited," in *Proc. Int. Conf. Comput. Sci. Appl. (ICCSA)*, 2008, pp. 1249–1259.

[14] H. S. Rhee, J. H. Park, W. Susilo, and D. H. Lee, "Improved searchable public key encryption with designated tester," in *Proc. 4th Int. Symp. ASIACCS*, 2009, pp. 376–379.

[15] K. Emura, A. Miyaji, M. S. Rahman, and K. Omote, "Generic constructions of secure-channel free searchable encryption with adaptive security," *Secur. Commun. Netw.*, vol. 8, no. 8, pp. 1547–1560, 2015.

[16] J. W. Byun, H. S. Rhee, H.-A. Park, and D. H. Lee, "Off-line keyword guessing attacks on recent keyword search schemes over

encrypted data," in *Proc. 3rd VLDB Workshop Secure Data Manage. (SDM)*, 2006, pp. 75–83.

[17] W.-C. Yau, S.-H. Heng, and B.-M. Goi, "Off-line keyword guessing attacks on recent public key encryption with keyword search schemes," in *Proc. 5th Int. Conf. ATC*, 2008, pp. 100–105.

[18] J. Baek, R. Safavi-Naini, and W. Susilo, "On the integration of public key data encryption and public key encryption with keyword search," in *Proc. 9th Int. Conf. Inf. Secur. (ISC)*, 2006, pp. 217–232.

[19] H. S. Rhee, W. Susilo, and H.-J. Kim, "Secure searchable public key encryption scheme against keyword guessing attacks," *IEICE Electron. Exp.*, vol. 6, no. 5, pp. 237–243, 2009.

[20] H. S. Rhee, J. H. Park, W. Susilo, and D. H. Lee, "Trapdoor security in a searchable public-key encryption scheme with a designated tester," *J. Syst. Softw.*, vol. 83, no. 5, pp. 763–771, 2010.

[21] L. Fang, W. Susilo, C. Ge, and J. Wang, "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," *Inf. Sci.*, vol. 238, pp. 221–241, Jul. 2013.

[22] I. R. Jeong, J. O. Kwon, D. Hong, and D. H. Lee, "Constructing PEKS schemes secure against keyword guessing attacks is possible?" *Comput. Commun.*, vol. 32, no. 2, pp. 394–396, 2009.

[23] R. Cramer and V. Shoup, "Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption," in *Proc. Int. Conf. EUROCRYPT*, 2002, pp. 45–64.