IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

TWINCRYPT SEARCHGUARD

Devansh Singh

Dept of CSE,ABES EC,Ghaziabad,India

Abstract – Ensuring data privacy in secure cloud storage has heightened interest in searchable encryption techniques. This study focuses on a critical cryptographic construct known as public key encryption with keyword search (PEKS), which plays a pivotal role in cloud storage applications. Traditional PEKS systems, however, are vulnerable to a significant security flaw known as the inside keyword guessing attack (KGA), where a malicious server exploits inherent weaknesses. To overcome this limitation, we introduce an enhanced PEKS model called dual-server PEKS (DS-PEKS). A key innovation in our framework is the introduction of a new type of smooth projective hash function (SPHF), termed linear and homomorphic SPHF (LH-SPHF). Leveraging LH-SPHF, we present a generic methodology for constructing a secure DS-PEKS scheme. To demonstrate the practicality of our approach, we provide an efficient implementation of the framework using a Decision Diffie-Hellman-based LH-SPHF and establish its robust security against KGA threats.

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

I. Introduction

Cloud computing refers to the delivery of computing resources, including hardware and software, as on-demand services over the internet. The term originates from the widespread use of a cloud-shaped icon to represent the intricate infrastructure involved in system diagrams. In this paradigm, users entrust their data, software, and computational needs to remote services managed by third-party providers. Cloud computing integrates hardware and software resources, providing users with access to powerful applications and robust server networks via the internet.

The cloud computing model is categorized into three primary service layers: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). These layers are complemented by an end-user layer that highlights the user's perspective in interacting with cloud services. For instance, users accessing the infrastructure layer can deploy their own applications on cloud resources, retaining responsibility for their maintenance and security. Conversely, applications accessed through the software layer are typically managed entirely by the service provider.

Benefits of Cloud Computing:

1. **Enhanced Efficiency**: Scale operations efficiently, achieving higher productivity with reduced workforce requirements, thereby lowering per-unit costs.
2. **Cost Savings**: Minimize technology infrastructure expenditures by adopting pay-as-you-go pricing models, reducing upfront investments.
3. **Global Accessibility**: Enable a distributed workforce to access resources globally, provided they have an internet connection.
4. **Process Optimization**: Accomplish tasks faster and more efficiently with streamlined workflows.
5. **Reduced Capital Investment**: Eliminate the need for significant expenditures on hardware, software, and licensing fees.
6. **Improved Accessibility**: Ensure easy, anytime, anywhere access to resources, simplifying operations and enhancing user convenience.

7. **Enhanced Project Management**: Monitor projects effectively, maintaining budgets and meeting timelines efficiently.
8. **Simplified Training**: Require minimal personnel training due to intuitive cloud interfaces and reduced hardware/software complexity.
9. **Minimized Licensing Costs**: Expand operations without the financial burden of acquiring additional software licenses.
10. **Greater Flexibility**: Adapt quickly to changing requirements without significant financial or personnel challenges.

For this study secondary data has been collected. From the website of KSE the monthly stock prices for the sample firms are obtained from Jan 2010 to Dec 2014. And from the website of SBP the data for the macroeconomic variables are collected for the period of five years. The time series monthly data is collected on stock prices for sample firmsand relative macroeconomic variables for the period of 5 years. The data collection period is ranging from January 2010 to Dec 2014. Monthly prices of KSE -100 Index is taken from yahoo finance.

II. EXISTING SYSTEM

In a Public Key Encryption with Keyword Search (PEKS) system, the sender encrypts specific keywords, known as PEKS ciphertexts, using the receiver's public key. These ciphertexts are attached to the encrypted data. To perform a keyword search, the receiver generates a trapdoor for the desired keyword and sends it to the server. By using the trapdoor and the PEKS ciphertext, the server can verify whether the keyword in the ciphertext matches the one specified by the receiver. If a match is found, the server provides the receiver with the corresponding encrypted data.Baek et al. introduced an innovative PEKS system that eliminates the need for a secure communication channel, referred to as Secure Channel-Free PEKS (SCF-PEKS)

III. PROPOSED SYSTEM

This paper makes four key contributions:

1. A novel framework named **Dual-Server Public Key Encryption with Keyword Search (DS-PEKS)** is introduced to address the security vulnerabilities inherent in traditional PEKS systems.
2. A new variant of the Smooth Projective Hash Function (SPHF), termed **linear and homomorphic SPHF (Lin-Hom SPHF)**, is proposed to support the construction of DS-PEKS.
3. A generic approach for building DS-PEKS using Lin-Hom SPHF is presented.
4. To demonstrate the practicality of the framework, we provide an efficient instantiation based on the Diffie-Hellman language.

1. Proposed Algorithm

The DS-PEKS scheme is defined using the following algorithms:

- **Setup(γ):** Takes the security parameter γ\gammaγ as input and outputs system parameters PPP.
- **KeyGen(P):** Accepts the system parameters PPP and generates public/secret key pairs for the front server (pkFS,skFS)(pk_{FS}, sk_{FS})(pkFS,skFS) and the back server (pkBS,skBS)(pk_{BS}, sk_{BS})(pkBS,skBS).
- **DS-PEKS(P, pkFS, pkBS, kw1):** Uses PPP, the front server’s public key pkFSpk_{FS}pkFS, the back server’s public key pkBSpk_{BS}pkBS, and a keyword kw1kw1kw1 to generate the PEKS ciphertext CTkw1CT_{kw1}CTkw1.
- **DS-Trapdoor(P, pkFS, pkBS, kw2):** Takes PPP, pkFSpk_{FS}pkFS, pkBSpk_{BS}pkBS, and a keyword kw2kw2kw2 to create the trapdoor Tkw2T_{kw2}Tkw2.
- **BackTest(P, skBS, CITS):** Accepts PPP, the back server’s private key skBSsk_{BS}skBS, and the internal testing state CITSCITSCITS to return a result of 0 or 1 based on the test outcome.

2. Implementation of Modules

The system implementation involves several key modules:

System Construction Module

This module involves setting up the required entities:

1. **Cloud User:** An individual or organization storing and accessing data on the cloud.
2. **Cloud Service Provider (CSP):** Manages cloud servers, offering storage as a service.

We propose the DS-PEKS framework, detailing its formal definition and security models. A variant of SPHF (Lin-Hom SPHF) is defined, enabling a generic DS-PEKS construction. Correctness analysis and security proofs are also provided, along with an efficient implementation.

Semantic Security Against Chosen Keyword Attack

This module ensures the system is semantically secure, preventing adversaries from distinguishing between keywords based on their corresponding PEKS ciphertexts. This ensures that ciphertexts reveal no information about the keywords.

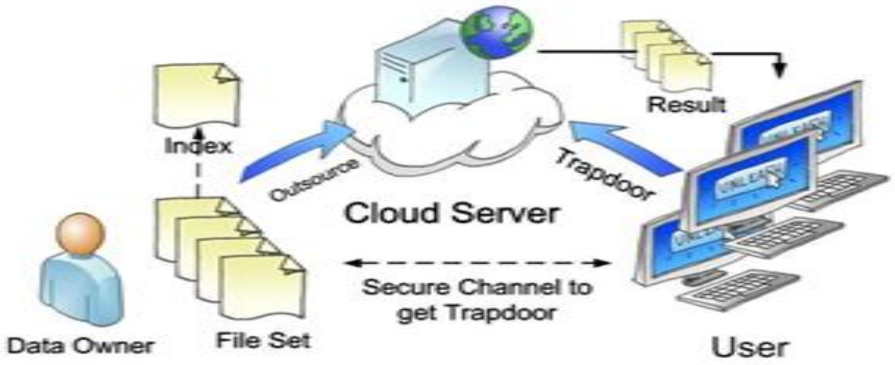
Front Server

The front server processes trapdoors and PEKS ciphertexts using its private key after receiving a query from the receiver. It forwards the internal testing states to the back server, ensuring that the trapdoors and ciphertexts remain concealed.

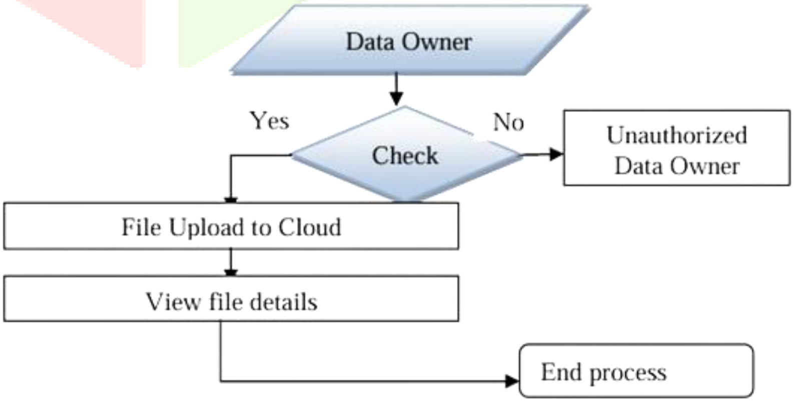
Back Server

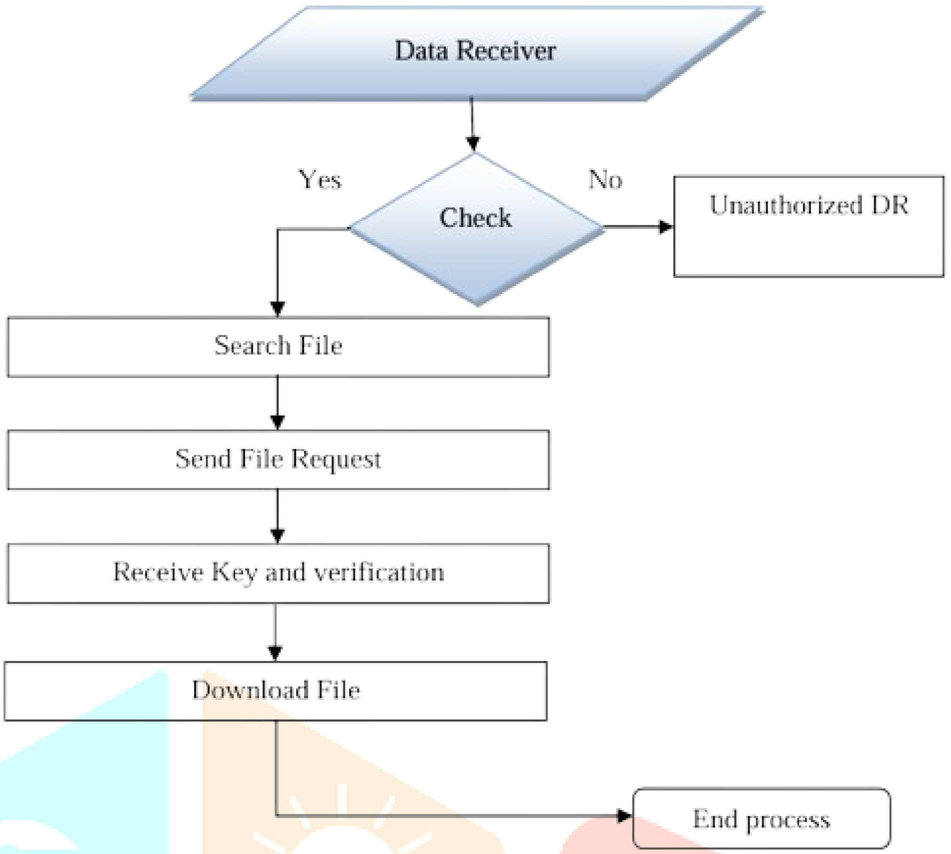
The back server identifies the queried documents by utilizing its private key along with the internal testing states received from the front server.

3. System Architectural Design Architecture Diagram:



User Interface: Data Flow Diagram:





IV.RELATED WORK

Cloud computing utilizes shared computing resources—both hardware and software—delivered as a service over a network, usually the Internet. The term originates from the cloud-shaped symbol often used in diagrams to represent complex infrastructure.

1. Tools and Technologies Used

The implementation of this project relies on the following technologies:

- **Java Technology:** A versatile platform encompassing a high-level programming language and execution environment.
- **SQL Server 2014:** A robust relational database management system used for efficient data management.

2. Literature Survey

The development of this project is informed by several significant contributions in the field of searchable encryption. Key works are summarized below:

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
- **Summary:** This paper introduces a new PEKS framework called Dual-Server Public Key Encryption with Keyword Search (DS-PEKS), which mitigates the risk of Keyword Guessing Attacks (KGA). The framework uses two non-colluding servers and employs a novel Smooth Projective Hash Function (SPHF) variant, providing enhanced security against KGAs.

b) Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions

- **Authors:** R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky
- **Summary:** This work advances Searchable Symmetric Encryption (SSE) by proposing stronger security definitions and more efficient constructions. The paper extends the traditional single-user setting to support multi-user scenarios, allowing multiple parties to perform secure queries over the same data.

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

- **Authors:** D. Khader
- **Summary:** This study explores a K-Resilient Public Key Encryption with Keyword Search (KR-PEKS) framework. The scheme improves upon existing PEKS designs by eliminating the need for secure channels and enabling multi-keyword searches. The approach leverages Identity-Based Encryption (IBE) to enhance key privacy.

d) Generic Constructions of Secure-Channel-Free Searchable Encryption with Adaptive Security

- **Authors:** K. Emura, A. Miyaji, M. S. Rahman, and K. Omote
- **Summary:** This paper extends secure-channel-free PEKS (SCF-PEKS) to an adaptive model, where adversaries can issue test queries dynamically. It introduces a generic construction using anonymous IBE and proposes an optimized version with reduced computational overhead.

e) Off-Line Keyword Guessing Attacks on Recent PEKS Schemes

- **Authors:** W.-C. Yau, S.-H. Heng, and B.-M. Goi
- **Summary:** The authors demonstrate vulnerabilities in SCF-PEKS and PKE/PEKS schemes. They reveal that offline keyword guessing attacks can compromise encrypted keywords when trapdoors are transmitted over public or secure channels.

V.CONCLUSION AND FUTURE SCOPE

In this work, we introduced a novel framework called **Dual-Server Public Key Encryption with Keyword Search (DS-PEKS)** to address the inherent vulnerabilities of traditional PEKS systems, particularly the risk of insider keyword guessing attacks. Our framework leverages two independent servers to enhance security, assuming they do not collude.

To support the DS-PEKS framework, we proposed a new variant of the **Smooth Projective Hash Function (SPHF)**, which enables the secure construction of a generic DS-PEKS scheme. We also provided an efficient instantiation of this SPHF, rooted in the Diffie-Hellman problem. This instantiation eliminates the need for computationally expensive pairings, resulting in a lightweight and efficient DS-PEKS implementation suitable for real-world applications.

Future Scope

1. **Optimization of Computational Efficiency:**
   Future research could focus on further reducing the computational overhead of DS-PEKS, particularly for resource-constrained environments like IoT and mobile devices.
2. **Support for Multi-Keyword Searches:**
   Extending the framework to support multi-keyword searches would improve its practicality for complex search queries in encrypted databases.
3. **Adaptability to Colluding Servers:**
   Enhancing the framework to provide security guarantees even when servers collude would make it more robust for highly adversarial environments.
4. **Integration with Real-World Systems:**
   Deploying and testing DS-PEKS in practical cloud storage systems could uncover performance bottlenecks and opportunities for further improvements.
5. **Incorporating Post-Quantum Cryptography:**
   With the advent of quantum computing, adapting the DS-PEKS framework to incorporate post-quantum cryptographic techniques would ensure its long-term viability.

By addressing these future challenges, the DS-PEKS framework can evolve into a comprehensive solution for secure keyword-based searches in encrypted cloud storage environments.

ACKNOWLEDGEMENT

I convey my thanks to my HOD Smt. Dr. Divya Mishra for providing me with help and support. I convey my sincere thanks to my guide Ms.Medha Malik 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] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

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

[8] 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.

[9] 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.

[10] 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.