INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN : 2454-9924

MULTI-KEYWORD SEARCHABLE ENCRYPTION SYSTEM FOR DISTRIBUTED SYSTEMS IN CLOUD TECHNOLOGY

C. Siva Kumar[1] Mr. N. Muni Sankar[2]

[1] Department of CSE, Sri Venkatesa Perumal College of Engineering and Technology, Tirupati, India, yic.siva@gmail.com

[2] Department of CSE, Sri Venkatesa Perumal College of Engineering and Technology, Tirupati, India ms.nagugari@gmail.com

Abstract: Given the widespread adoption of cloud storage in a variety of applications, how to preserve data privacy while allowing efficient data search and retrieval in a distributed context remains a difficult research challenge. Existing searchable encryption systems are still insufficient in terms of intended functionality as well as security and privacy. The most difficult problems include providing multi-keyword search in a multi-user environment, masking search and access patterns, and preventing keyword guessing assaults (KGA). We introduce a novel searchable encryption strategy in this application that overcomes all of the above issues at once, making it viable to use in distributed systems. It not only allows for multi-keyword searches over encrypted data in a multi-writer/multi-reader environment, but it also ensures the anonymity of the data and search patterns. We leave developing a secure SE-EPOM with fewer rounds of communication between CP and IS to provide higher security.

Keywords: Searchable Encryption, Multi-Keyword Search, Multi-User Access, Search Pattern, Access Pattern.

1. Introduction

Due to its compelling advantages over traditional data storage, cloud storage has become one of the most popular and vital cloud services for both industrial and personal customers since the development of cloud computing. By 2021, the global data center storage capacity is expected to reach 2,300 exabytes, according to Statista, a statistics portal website.

With the fast rise of cloud storage, data security and privacy are critical factors that must be addressed properly to avoid financial loss or reputational damage as a result of cloud data leaks. As a result, it's only natural to use cryptographic measures like data encryption algorithms to protect sensitive data stored in the cloud. However, such a simple privacy protection strategy does not work for large cloud storage facilities since it prevents the cloud server from doing a quick search of the stored data in response to a user request.

The concept of Public-key Encryption with Keyword Search (PEKS) was developed in the seminal work of Bone et al. There are three entities in a PEKS scheme: a data owner (or writer), a data user (or reader), and a storage server. To send data to a user via the storage server, the owner extracts a keyword from the data and then encrypts the keyword (known as a searchable ciphertext) using the intended user's public key. The server receives the actual data, which might be encrypted individually, as well as its searchable ciphertext.

Then, using his or her private key and a phrase of interest, only the intended user can produce a search token (a.k.a. trapdoor) and transmit it to the server, which will check whether the trapdoor matches a searchable ciphertext and inform the user of the search result. If the owner wants to share the same data with other users in this approach, he or she must repeat the aforementioned action and generate several searchable ciphertexts, which is not feasible or scalable in dispersed contexts.

To fend off KGA attacks, various techniques have been offered. KGA can be defeated in two ways: by preventing the server from generating searchable ciphertext on its own and then launching KGA; and by disabling public testing. The first method has resulted in the development of new cryptographic primitives such as public-key authenticated encryption with keyword search (PAEKS), in which the data owner's private key is used to construct and authenticate the searchable ciphertext. PAEKS, on the other hand, uses the data user's public key to construct the searchable ciphertext, hence it doesn't support multi-user search.

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN : 2454-9924

Because everyone nowadays has access to a cell phone, we devised an automated method in which farmers may submit images of diseased leaves to our server, where a neural network will identify the disease and the disease classification, as well as the solution, will be provided back to the farmer. We proposed the architecture for the automated system's disease classification section in this paper. We have created a deep learning strategy using our rice disease dataset that we have collected over the past several months, inspired by work on convolutional neural networks.

2. Related Works

Multi-Writer Searchable Encryption, commonly known as public-key encryption with keyword search (PEKS), is useful for a variety of data sharing scenarios. It allows users to browse through encrypted material that has been encrypted with various keys. However, most existing PEKS techniques are based on traditional security assumptions, which have been shown to be insufficient to counteract the dangers posed by quantum computers. In this research, we present a lattice-based searchable encryption system based on the learning with errors (LWE) hardness assumption to address the aforementioned problem. In particular, we notice that in a simple scheme, each user's keys are made up of big matrices and the lattice's basis. Our approach is meant to allow users to directly use their identity for data encryption, reducing the burden of key management. To make our idea nearly practicable, we propose many optimization strategies for implementation. To be sure, we run our method through thorough security, complexity, and parameter analyses, as well as exhaustive tests on a commodity machine.

Because of its high efficiency, symmetric key encryption is commonly employed to encrypt files in cloud data storage systems. Searchable symmetric encryption (SSE) [2], has been proposed to allow an untrusted/semi-trusted cloud storage server to search encrypted data while maintaining data confidentiality. A typical SSE strategy involves a user storing encrypted files on a cloud storage server and afterwards retrieving encrypted files containing particular keywords. The main security criterion of SSE is that throughout the search process, the cloud server knows nothing about the files or keywords.

Both academic and industrial researchers have looked into Searchable Encryption (SE) extensively. While many academic SE systems demonstrate provable security, in order to achieve high performance, they often leak certain query information (e.g., search and access patterns). Several inference attacks have taken advantage of this leakage, for example, a query recovery attack can turn opaque query trapdoors into their corresponding keywords based on past knowledge. Many proposed [3] SE methods, on the other hand, would necessitate extensive change of existing applications, making them less feasible, usable, and deployable.

In the cloud era, how to efficiently search across encrypted data is a critical and fascinating subject. In 2004, bone et al [4]. proposed the concept of public key encryption with keyword search (PEKS) to overcome the problem. In practically all PEKS techniques, however, an inside opponent may recover the keyword from a particular trapdoor by guessing the keywords exhaustively offline. It's still a challenge to defend against the inside keyword guessing assault in PEKS.

We study a class of public key encryption algorithms that support plaintext equality testing and user-specified authorization in this work. Two users with their own public/private key pairs can send tokens to a proxy to authorize it to run plaintext equality tests from their ciphertexts using this new primitive. In our security model, we propose an architecture with provable security and a formal description for this primitive. We improve the proposed cryptosystem by using the concept of computational client puzzles to alleviate the dangers posed by semi trusted proxies.

Author & Year	Proposed	Finding/Outcomes
L. Xu, X. Yuan, R. Steinfeld, C. Wang, and C. Xu	from the learning with errors (LWE) hardness assumption, a lattice-based searchable encryption scheme	It gives the detailed overview of the LWE encryption.
X. Liu, G. Yang, Y. Mu, and R. Deng	In proposed searchable symmetric encryption (SSE) has been proposed.	Explains about the SSE encryption
G. Wang,	The secure and practical	Overview of searchable

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

C. Liu, Y. Dong, P. Han, H. Pan, and B. Fang	searchable symmetric encryption	symmetric encryption.
Q. Huang and H. Li	The propose introduce the notion of Public-key Authenticated Encryption with Keyword Search (PAEKS) to solve the problem	Overview of the Encryption and decryption.
K. Huang, R. Tso, and Y.-C. Chen	In this we proposed cryptosystem algorithm	An algorithm is proposed which is used to encrypt and decryption

Table 1: Related Works Summary

3. Methodology

The procedure to develop our system is clearly described in this section.

- To develop this application first we need to install the database server for the execution.
- For backend process here we use python language.
- For front end, HTML, CSS are used to design the website.
- For database purpose we use SQL.
- For the process building we create a different modules, admin, user and owner.

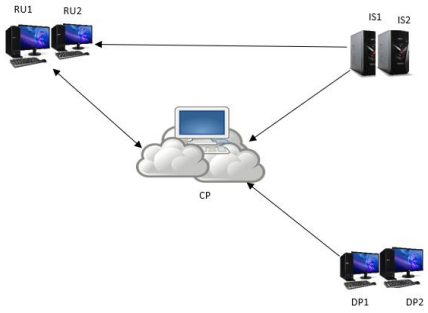

Fig: Block Diagram

AES Algorithm:

ISSN : 2454-9924

AES stands for (Advanced Encryption Standard). The encryption procedure employs a set of round keys, which are uniquely derived keys. These are applied to an array of data that contains exactly one block of data, along with other operations? The information that will be encrypted. This array is referred to as the state array.

For a 128-bit block, you perform the following aes encryption steps:

From the cypher key, create a series of round keys.

Use the block data to populate the state array (plaintext).

To the starting state array, append the initial round key.

Nine rounds of state manipulation are required.

The tenth and final phase of state manipulation should be completed.

Make a copy of the final state array as encrypted data (ciphertext).

Because the tenth round includes a somewhat different manipulation than the others, the rounds are given as "nine followed by a final tenth round."

The block to be encrypted is simply a 128-bit sequence. Because AES works in byte increments, we must first divide the 128 bits into 16 bytes. We say "convert," but it's almost definitely already saved in this format. RSN/AES uses a two-dimensional byte array with four rows and four columns for operations. The 16 bytes of data at the start of the encryption.

4. Results and Discussion:

The proposed mechanism provides the basis for enabling multi-keyword search encryption methodology. By applying SE-EPOM scheme in proposed method number of authentication rounds are reduced due to the elimination of key generation center (KGC). Hence doe to the elimination of KGC data can be easily transferred between CP and IS's. By using the proposed method, we obtain the below results.

Home Page:

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN : 2454-9924

Fig1: Home page

Registration Page:

Fig2: Registration page

Login Page:

Fig3: Registration page

Data upload:

Fig4: Files Upload

View Data:

Fig5: View Data

Download Data:

Fig6: Data Download

Conclusion:

The evaluation on compared schemes and our scheme shows that the overall performance of our distributed SEEPOM scheme outperforms other solutions. We leave designing a secure SE-EPOM with fewer rounds of communication between CP and IS's as our future work. We successfully proved that our proposed system gives optimum results.

References

[1] "Forecast number of personal cloud storage consumers/users worldwide from 2014 to 2020 (in millions)," https://www.statista.com/statistics/638593/ worldwide-data-center-storage-capacity-cloud-vs-traditional/, accessed August 30, 2018.

[2] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in international conference on the theory and applications of cryptographic techniques, 2004, pp. 506–522.

[3] 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 Workshop on Secure Data Management, 2006, pp. 75–83.

[4] Q. Huang and H. Li, "An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks," Information Sciences, vol. 403, pp. 1–14, 2017.

ISSN : 2454-9924

[5] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on, 2000, pp. 44–55.

[6] E.-J. Goh et al., "Secure indexes." IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.

[7] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions,"JournalofComputerSecurity, vol. 19, no. 5, pp. 895–934, 2011.

[8] K. Kurosawa and Y. Ohtaki, "Uc-secure searchable symmetric encryption," in International Conference on Financial Cryptography and Data Security, 2012, pp. 285–298.

[9] P. Wang, H. Wang, and J. Pieprzyk, "Keyword field-free conjunctive keyword searches on encrypted data and extension for dynamic groups," in international conference on cryptology and network security, 2008, pp. 178–195.

[10] B. Zhang and F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 262–267, 2011.

[11] K. Huang, R. Tso, and Y.-C. Chen, "Somewhat semantic secure public key encryption with filtered-equality-test in the standard model and its extension to searchable encryption," Journal of Computer and System Sciences, vol. 89, pp. 400–409, 2017.

[12] G. Wang, C. Liu, Y. Dong, P. Han, H. Pan, and B. Fang, "Idcrypt: A multi-user searchable symmetric encryption scheme for cloud applications," IEEE Access, vol. 6, pp. 2908–2921, 2018.

[13] X. Liu, G. Yang, Y. Mu, and R. Deng, "Multi-user verifiable searchable symmetric encryption for cloud storage,"IEEE Transaction Dependable and Secure Computing, 2018.

[14] A. Fiat and M. Naor, "Broadcast encryption," in Annual International Cryptology Conference, 1993, pp. 480–491.

[15] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Ros¸u, and M. Steiner, "Highly-scalable searchable symmetric encryption with support for Boolean queries,"inAnnualCryptologyConference, 2013, pp. 353–373.