Novel approach for Secure Cloud Storage with Similar word Search

O. Naga Kumari[1], Samidi Sindhuja[2], S.Haripriya[2], G. Shireesh Goud[2]

[1]Assistant Professor in Department of Information Technology .in Teegala Krisha Reddy Engineering college, Telangana, India

[2]UG Scholar in Department of Information Technology .in Teegala Krisha Reddy Engineering college, Telangana, India

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 ,encryption with similar word search ,which is very useful in many applications of cloud storage. Unfortunately, it has been shown that the traditional ,framework suffers from an inherent insecurity called inside similarword guessing attack ,launched by the malicious server. To address this security vulnerability, we propose a new ,framework named dual-server similar. As another main contribution, we define a new variant of the smooth projective hash functions ,referred to as linear and homomorphic We then show a generic construction of secure DS- ,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.

Keywords: Similarword search, secure cloud storage, encryption, inside similarword guessing attack, smooth projective hash function, Diffie-Hellman language.

I. INTRODUCTION

Cloud storage outsourcing has become a popular application for enterprises and organizations to reduce the burden of maintaining big data in recent years. However, in reality, end users may not entirely trust the cloud storage servers and may prefer to encrypt their data before uploading them to the cloud server in order to protect the data privacy.

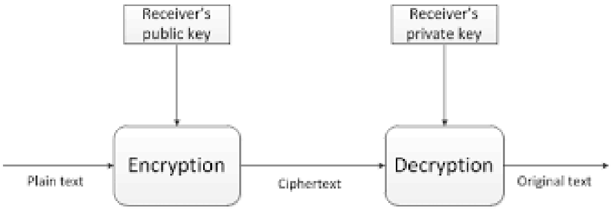

Figure 1. General view of security in text.

This usually makes the data utilization more difficult than the traditional storage where data is kept in the absence of encryption. One of the typical solutions is the searchable encryption which allows the user to retrieve the encrypted documents that contain the user-specified similarwords, where given the similar word trapdoor, the server can find the data required by the user without decryption. Given the trapdoor and the , ciphertext, the server can test whether the similar word underlying the ,ciphertxt is equal to the one selected by the receiver.

Simply improving the physical security of the trash is not sufficient to guard against theft of plaintext. In today's world, most plaintext is stored digitally and is open to theft via portable media or online hacking. As a result, implementing local procedures to guard against unauthorized removal of portable media and proper disposal of legacy disk drives and discarded computers is another key to preventing theft and possibly compromise of plaintext data that may contain sensitive or privileged information.

II. MOTIVATION

Despite of being free from secret, distribution, ,schemes suffer from an inherent insecurity regarding the trapdoor similarword privacy, namely *inside Similarword Guessing Attack* similar. The reason leading to such a security vulnerability is that anyone who knows receiver's public ,can generate the ,ciphertext of arbitrary similar word himself. Specifically, given a trapdoor, the adversarial server can choose a guessing similar word from the similar word space and then use the similar word to generate a ,cipher text. The server then can test whether the guessing similar word is the one underlying the trapdoor. This *guessing-then-testing* procedure can be repeated until the correct similarword is found. Such a guessing attack has also been considered in many password-based systems.

III. PROPOSAL OVER VIEW

Step for formalizing the text:

1. server security issues.
2. framing the functions
3.construction of key generic function.
4.Initiation of text encryption.

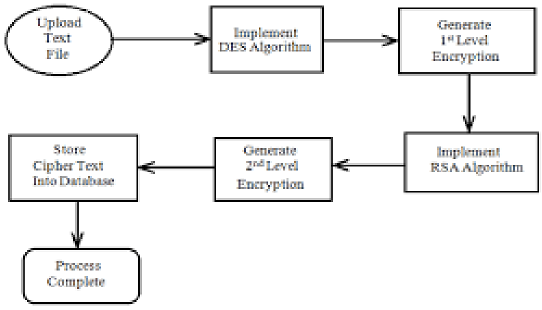

Fig. 3. Block Diagram of Multilevel Encryption

Figure 2. illustration of function execution.

Security Models

In this subsection, we formalise the following security models for a DS-,scheme against the adversarial front and back servers, respectively.One should note that both the front server and the back server here are supposed to be "honest but curious" and will not collude with each other. More precisely, both the servers perform the testing strictly following the scheme procedures but may be curious about the underlying similarword. We should note that the following security models also imply the security guarantees against the outside adversaries which have less capability compared to the servers.

In cryptography, ciphertext or cyphertext is the result of encryption performed on plaintext using an algorithm, called a cipher.[1] Ciphertext is also known as encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer without the proper cipher to decrypt it. Decryption, the inverse of encryption, is the process of turning ciphertext into readable plaintext. Ciphertext is not to be confused with codetext because the latter is a result of a code, not a cipher.

- Private-key cryptography (symmetric key algorithm): the same key is used for encryption and decryption
- Public-key cryptography (asymmetric key algorithm): two different keys are used for encryption and decryption

In a symmetric key algorithm (e.g., DES and AES), the sender and receiver must have a shared key set up in advance and kept secret from all other parties; the sender uses this key for encryption, and the receiver uses the same key for decryption. In an asymmetric key algorithm (e.g., RSA), there are two separate keys: a *public key* is published and enables any sender to perform encryption, while a *private key* is kept secret by the receiver and enables only him to perform correct decryption.

Symmetric key ciphers can be divided into block ciphers and stream ciphers. Block ciphers operate on fixed-length groups of bits, called blocks, with an unvarying transformation. Stream ciphers encrypt plaintext digits one at a time on a continuous stream of data and the transformation of successive digits varies during the encryption process.

- Ciphertext-only: the cryptanalyst has access only to a collection of ciphertexts or codetexts
- Known-plaintext: the attacker has a set of ciphertexts to which he knows the corresponding plaintext
- Chosen-plaintext attack: the attacker can obtain the ciphertexts corresponding to an arbitrary set of plaintexts of his own choosing
    - Batch chosen-plaintext attack: where the cryptanalyst chooses all plaintexts before any of them are encrypted. This is often the meaning of an unqualified use of "chosen-plaintext attack".
    - Adaptive chosen-plaintext attack: where the cryptanalyst makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions.
- Chosen-ciphertext attack: the attacker can obtain the plaintexts corresponding to an arbitrary set of ciphertexts of his own choosing
    - Adaptive chosen-ciphertext attack
    - Indifferent chosen-ciphertext attack
- Related-key attack: like a chosen-plaintext attack, except the attacker can obtain ciphertexts encrypted under two different keys. The keys are unknown, but the relationship between them is known; for example, two keys that differ in the one bit.

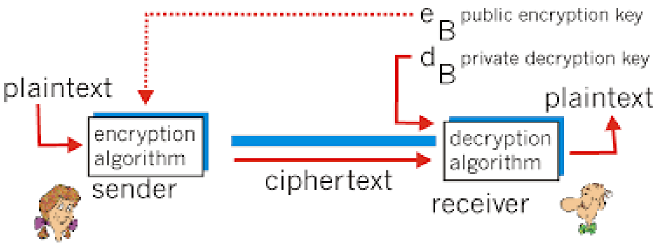

Figure 3. Cyphertext modulation in each phase of function evaluation.

our scheme is the most efficient in terms of ,computation. It is because that our scheme does not include pairing computation. Particularly, the scheme requires the most computation cost due to 2 pairing computation per ,generation. As for the trapdoor generation indicated in Figure 8, as all the existing schemes do not involve pairing computation, the computation cost is much lower than that of ,generation. It is worth noting that the trapdoor generation in our scheme is slightly higher than those of existing schemes due to the additional exponentiation computations. When the searching similarword number is 50, the total computation cost of our scheme is about 0.25 seconds.As illustrated in figure, the each scheme of cost the most time due to an additional pairing computation in the exact testing stage. One should note that this additional pairing computation is done on the user side instead of the server. Therefore, it could be the computation burden for users who may use as a Computation cost of testing in different schemes. light device for searching data. In our scheme, although we also require another stage for the testing, our computation cost is actually lower than that of any existing scheme as we do not require any pairing computation and all the searching work is handled by the server.

Cryptanalysis is the study of methods for obtaining the meaning of encrypted information, without access to the secret information that is normally required to do so. Typically, this involves knowing how the system works and finding a secret key. Cryptanalysis is also referred to as codebreaking or cracking the code. Ciphertext is generally the easiest part of a cryptosystem to obtain and therefore is an important part of cryptanalysis. Depending on what information is available and what type of cipher is being analyzed, crypanalysts can follow one or more attack models to crack a cipher.

Cipher is an algorithm which is applied to plain text to get ciphertext. It is the unreadable output of an encryption algorithm. The term "cipher" is sometimes used as an alternative term for ciphertext. Ciphertext is not understandable until it has been converted into plain text using a key.

Earlier cipher algorithms were performed manually and were entirely different from modern algorithms which are generally executed by a machine. Different types of ciphers exist, some of which are:

Substitution Cipher: This offers an alternative to the plaintext. It is also known as Caesar cipher.

Polyalphabetic Substitution Cipher: In this cipher, a mixed alphabet is used to encrypt the plaintext, but at random points it would change to a different mixed alphabet which indicates the change with an uppercase letter in the Ciphertext.

Transposition Cipher: This cipher is also known as Rail Fence Cipher and is a permutation of the plaintext.

Permutation Cipher: The positions held by plaintext are shifted to a regular system in this cipher so that the ciphertext constitutes a permutation of the plaintext.

Private-key Cryptography: In this cipher, even the attacker is aware of the plaintext and corresponding ciphertext. The sender and receiver must have a pre-shared key. The shared key is kept secret from all other parties and is used for encryption as well as decryption. DES and AES algorithms are examples of this type of cipher. This cryptography is also known as "symmetric key algorithm".

Public-key Cryptography: In this cipher, two different keys - public key and private key - are used for encryption and decryption. The sender uses the public key to perform encryption, whereas the receiver is kept in the dark about the private key. This is also known as asymmetric key algorithm.

IV. CONCLUSIONS

In this paper, we proposed a new framework, named Dual-Server Public ,Encryption with Similarword Search similar, that can prevent the inside similarword guessing attack which is an inherent vulnerability of the traditional ,framework. We also introduced a new Smooth Projective Hash Function (SPHF) and used it to construct a generic DS-,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-,scheme without pairings.

V. REFERENCES

[1]. R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang,"A new generalframework for secure public ,encryption with similarword 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 searcheson encrypted data," in Proc. IEEE Symp. Secur. Privacy, May 2000,pp. 44–55. R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu,"Order preservingencryption for numeric data," in Proc. ACM SIGMOD Int. Conf. Manage.Data, 2004, pp. 563–574.

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

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

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

[6]. 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.

[7]. 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.

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

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

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