International Journal of Engineering & Technology, *7 (3.29) (2018) 694-696*

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Secure Full-Text Retrieval on Cloud

B. Deepthi [1*] , Rakesh [2]

[1] Assistant Professor, [2]UG Student
[1,2] Dept of Computer Science Engineering, BVRIT Narsapur
**Corresponding Author E-mail: deepthiraya@gmail.com*

Abstract

Cloud Computing is a present day technology that effectively support the client oriented services. These days we are mostly using applications that consumes the cloud storage for storing and retrieving information. In such case that data management and privacy preservation cryptographic technique the data is converted to unreadable format. Due to this full text retrieval on encrypted data on cloud of required information becomes complex. Therefore in this paper we proposed bit slice indexing method on Elliptic-Curve-Diffie-Hellman for providing some security to cloud.

Keywords:

1. Introduction

Cloud computing has been widely recognized as a capable solution for large data processing, as it claims that the need of maintaining dedicated and expensive computing hardware and software can be eliminated [1]. The key to make this true in practice is that cloud computing supports providing massive computing infrastructure, platform and software resources as services and enables the users to pay only for the resources and services they use [2]. Cloud computing has become popular recently due to several advantages over traditional computing models. Typical advantages include flexibility, scalability, agility, energy efficiency and cost saving [3]. The organizations are forced to keep data or information in an environment which is easily accessible by the stake holders or authorized persons. In such situations, the suitable solution is to store data in a cloud environment. This can be achieved by ensuring that the right personnel are accessing the information. Cloud Service Providers (CSPs) provide identity and other kinds of access management for the customers in their cloud infrastructure [4]. But, the cloud, as a semi-trusted entity, is not fully trusted by its customers usually due to many reasons. Besides, the database may contain some sensitive information, such as costumer privacy and business secrets [5]. Thus, cloud customers are usually reluctant to outsource their sensitive data to cloud in the form of plaintext [6]. Encryption is a good way for users to guarantee data confidentiality. But classical cryptographic primitives will cause some essential data utilization services based on plaintext to be inapplicable. In the cloud environment, data owners usually share their outsourced documents with other data users. Faced with the massive data, users tend to search specific keyword to get their target documents.

The most helpful method to address the problem is searchable encryption which allows users to selectively retrieve documents of interest from the cloud through a keyword-based search technology [7]. Searchable encryption schemes have been developed in recent years for balancing search efficiency and data security. However, the existing approaches mainly focus on keyword-based search which is difficult to meet the requirements of the large scale cloud storage systems [8]. Majority of work in this area assumes that the cloud server is honest-but-curious. To safely transmit the data through the cloud servers, encryption and decryption techniques are used. Data owners will encrypt the data using any of the encryption algorithm and will forward to the cloud servers. The encrypted data will be stored in the cloud databases from which the data will be accessed by the users by using the same decryption techniques [9]. This encryption algorithm consists of key generation, public key and private key. Public key will be shared to the cloud servers to receive and forward the data. Private Key will be shared to the respective users and they will decrypt the data using the private key. After encryption the data will be transmitted to the cloud servers where the data will be inaccessible but could be transmitted to the respective users using specific searching method [10]. In this proposed methodology, bit slice indexing based ECDH algorithm for encrypting the data. The bit slice index method is used to retrieval the data from the cloud storage for the user. Therefore, we design a bit slice index structure without word offset position to achieve the secure and efficient full-text retrieval over the cloud encrypted data.

2. Literature Review

C. Y. Yang, et al., [11] proposed a scheme in cloud service applied to smart home systems based on the IoT and the key technologies include sensing technology and cloud computing ability. The method provided a platform to prevent collusion between users and the Cloud Service Provider (CSP). The method protected the privacy of the checked data, and avoided the leakage of personnel information in the protocol. The method minimized the computational cost incurred through the application of bilinear pairings. The method only considered the users belong to the same groups and the number of users must be more than two.

H. Cui,et al., [12] presented an attribute-based cloud storage system with secure provenance by supporting dynamic user management. The method enabled fine-grained access control, and reduced too much performance overhead. The method supported data provider anonymity and traceability by authority and provided secure data provenance. The method did not support user revocation and the technique was started with providing a concrete construction. The revocation was extended by the method with the revocation functionality. The performance of the method was not evaluated by the experimental studies which was a major drawback of the technique.

Mehmet SabırKiraz, [13] highlighted the main security issues for the cloud services and deployment models. The main security problems in cloud computing was classified into data security and privacy, data storage security and adversarial attacks. The modern cryptographic mechanisms were expected to enhance data privacy and strengthen the security of cloud computing. The paper described various technological solutions, research goals of short and long term of the cloud security was well addressed by using classical cryptographic mechanisms. The paper explored the new directions in cloud computing security, while highlighting the correct selection of the fundamental technologies from cryptographic view.

D. He,et al., [14] proposed a Privacy-Preserving Certificate Less Provable Data Possession (PP-CLPDP) scheme to address certificate management and key escrow problems as well as ensured the privacy protection. The paper presented a security model for CLPDP scheme, which built on the security model. The method also presented a PP-CLPDP scheme for public cloud storage, based on bilinear pairings. The implementation of the scheme demonstrated the potential for the scheme to be deployed in a public cloud storage service and providing data integrity for big data. The PP-CLPDP scheme had less computation overhead when generating tags and checking the data integrity.

W. Teng, et al., [15] proposed a hierarchical attribute-based access control scheme with constant-size ciphertext for access control in cloud storage systems. The length of the ciphertext and the number of bilinear pairing evaluations to a constants were fixed, hence the scheme was fixed. The hierarchical authorization structure of the scheme reduced the burden and risk of a single authority scenario. The computational cost in encryption and decryption algorithm was low. The experimental results showed that the scheme was efficient, scalable and fine-grained in dealing with access control for outsourced data in cloud computing. The method was more complex and less efficient for access control in a cloud environment.

3. Proposed Work:

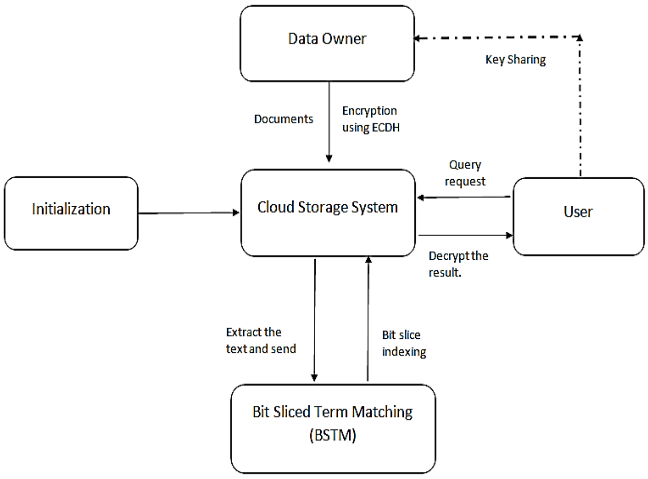
This paper includes involved work and identified issues in system in addition to that an optimum solution is also provided. Cloud Computing the name itself indicates that it provides support for effective computing and enables to provide the storage solutions at the remote end.

1. Data Security
2. Data Owner and Client Privacy Management
3. Searchable Data Space

In this we are going to look at few security algorithms like,

1. Initialization
2. Key Sharing
3. Encryption
4. Bit Sliced Term
5. Decryption

3.1. Block Diagram



4. Proposed Methodology

The proposed method consists of four polynomial algorithms as follows:

✓ Initialization (Setup):

- The cloud server creates all the index nodes and the inner links between the index nodes, before the cloud server provides the storage services to the users.
- Setup (1k) will take implicit security parameter k and output public parameter MPK and master key MSK.

✓ Key Sharing :

- The key generation process (KeyGen) is done by using key generation algorithm, before the process of sharing the key.
- The generation of the secret key SK is done by an algorithm called Central Authority (CA), takes as input the master key of CA and the set of attributes S for user.
- The secret key is shared among the data owner and the user.

✓ Encryption :

- The data owner sends the documents to the cloud storage system for encryption process.
- The encryption algorithm called Bit Sliced Indexing based Elliptical Curve Diffie-Hellman (ECDH).
- The algorithm ECDH takes as input the message M, public parameter MPK and access structure A over the universe of attributes.
- The users had a valid set of attributes which satisfy the access policy can only able to decrypt for the generation of output CipherText (CT).
- The method assumed that the CT implicitly contains access structure A.

✓ Bit Sliced Term Matching (BSTM) :

- The user given a query Q with a list of keyword values Q = <keyword-1, keyword-2.., keyword-|Q|>, which are expected to appear in a multi-valued keyword column K of an object-relational table T.
- The method used to find the set of k rows that have the largest number of matching keywords with the query list Q.
- The list denote the bitmap representing rows of table T that contains keyword-i in its column K by Bi; these bitmaps will occur as terms of an index KX.
- The task to find the Ordinal positions which have the largest number of matching 1's among all bitmaps B1, B2.., Bm.
- The indexing values send to the cloud storage system which is found by the algorithm called BSTM.

✓ Decryption :

- The user send a query request to cloud storage for decrypting the documents sent by the data owner.

- The decrypt algorithm run by user takes input the public parameter MPK, the CT contains access structure A and the secret key SK containing attribute set S.
- If S satisfies the access tree then algorithm decrypt the CT and give M otherwise gives"∅ ".
- The decrypted result again sent to the user from the cloud storage system.

5. Conclusion and Future Work:

The main aim of this paper is to discuss about the most trending topic these days that is Cloud Computing. First of all for any new application or technology security is the basic thing to avoid data loss to third party. Hence this paper mainly focuses on the steps of bit slice indexing method on ECDH algorithms that will enhance to improve the performance on Query Precision, Query Time, Time Cost and Index Storage Space.

Future work can be carried out with experimental results and shows the efficiency of our solution. We will continue on the privacy and security parameters for efficient searchable encryption schemes. Hence in the future, the clients we use will be genuine thin clients, which we just use by a little configuration. IOT will produce immensely huge data which we would store in cloud and big data systems.

Reference

[1] W. Zheng, Y. Qin, B. Emmanuel, D. Zhang, and J. Chen, “Cost optimization for deadline-aware scheduling of big-data processing jobs on clouds”, Future Generation Computer Systems, 2017.

[2] N. Sachdeva, O. Singh, P. K. Kapur, and D.Galar, “Multi-criteria intuitionistic fuzzy group decision analysis with TOPSIS method for selecting appropriate cloud solution to manage big data projects”, International Journal of System Assurance Engineering and Management, vol. 7, no. 3, pp. 316-324, 2016.

[3] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, “A secure cloud computing based framework for big data information management of smart grid”, IEEE transactions on cloud computing, vol. 3, no. 2, pp. 233-244, 2015.

[4] Indu, PM Rubesh Anand, and Vidhyacharan Bhaskar. "Encrypted Token based Authentication with Adapted Security Assertions Mark-up Language Technology for Cloud Web Services." Journal of Network and Computer Applications, 2017.

[5] Lu. Zhou,Youwen Zhu, and Aniello Castiglione. "Efficient k-NN query over encrypted data in cloud with limited key-disclosure and offline data owner." Computers & Security, 2016.

[6] H. Yin, Z. Qin, L. Ou, and K. Li, “A query privacy-enhanced and secure search scheme over encrypted data in cloud computing”, Journal of Computer and System Sciences, 2017.

[7] X. Jiang, J. Yu, J. Yan, and R. Hao, “Enabling efficient and verifiable multi-keyword ranked search over encrypted cloud data”, Information Sciences, vol. 403, pp. 22-41, 2017.

[8] W. Song, B. Wang, Q. Wang, Z. Peng, W. Lou, and Y. Cui, “A privacy-preserved full-text retrieval algorithm over encrypted data for cloud storage applications”, Journal of Parallel and Distributed Computing, vol. 99, pp. 14-27, 2017.

[9] R. Pitchai, S. Jayashri, and J. Raja. "Searchable Encrypted Data File Sharing Method Using Public Cloud Service for Secure Storage in Cloud Computing." Wireless Personal Communications, vol. 90, no. 2, pp. 947-960, 2016.

[10] Wang, Haijiang, Xiaolei Dong, and Zhenfu Cao. "Secure and efficient encrypted keyword search for multi-user setting in cloud computing." Peer-to-Peer Networking and Applications, pp. 1-11, 2017.

[11] C. Y. Yang, C. T. Huang, Y. P. Wang, Y. W. Chen, and S. J. Wang, “File changes with security proof stored in cloud service systems”, Personal and Ubiquitous Computing, pp. 1-9, 2017.

[12] H. Cui, Robert H. Deng, and Yingjiu Li. "Attribute-based cloud storage with secure provenance over encrypted data." Future Generation Computer Systems, vol. 79, pp. 461-472, 2018.

[13] Mehmet SabırKiraz, "A comprehensive meta-analysis of cryptographic security mechanisms for cloud computing", Journal of Ambient Intelligence and Humanized Computing, vol. 7, no. 5, pp. 731-760, 2016.

[14] D. He, N. Kumar, H. Wang, L. Wang, and K. K. R. Choo, “Privacy-preserving certificateless provable data possession scheme for big data storage on cloud”, Applied Mathematics and Computation, vol. 314, pp. 31-43, 2017.

[15] W. Teng, G. Yang, Y. Xiang, T. Zhang, and D. Wang, “Attribute-based access control with constant-size ciphertext in cloud computing”, IEEE Transactions on Cloud Computing, 2015.