International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 3 229 – 231

Efficient Fine Grained Access Control with Semantic Keyword Search on Encrypted Cloud Storage

Mr. D. Maria Manuel Vianny,
Computer Science and Engineering,
UCE-Thirukkuvalai,
Nagapattinam,India.
viannycse@gmail.com

M. Nithya,
Computer Science and Engineering,
UCE-Thirukkuvalai,
Nagapattinam,India.
nithyamanikkam96@gmail.com

R. Bhuvaneshwari,
Computer Science and Engineering,
UCE-Thirukkuvalai,
Nagapattinam,India.
bhuvanakarthika65@gmail.com

B.Priyanga,
Computer Science and Engineering,
UCE-Thirukkuvalai,
Nagapattinam, India.
bpriyangapriya007@gmail.com

G. Gnanapriya,
Computer Science and Engineering,
UCE-Thirukkuvalai,
Nagapattinam, India.
s.gnanasambantham96@gmail.com

Abstract—Using cloud computing, multi data owner can store their data on remote servers and allow data access to private users through the cloud servers.The cloud characteristics are on-demand self-service, location independent network access, ubiquitous network access and usage based pay. Due to this charming features private and public organization are outsourcing their large amount of data on cloud storage. First, we introduce in the cloud framework for multi data owners. Multi data owners upload the files in encrypted form using ECC algorithm. User can register the aadhar card number to the cloud multi data owner. The multi data owner can generate the two keys to allow access the data. User can request to multi data owner. Cloud data storage can provide the encrypted data. This encrypted data is strong protection for data backup and recovery purposes. There are two keys are used in the plaintext form to be converted in the cipher text form. Another key will generate and converted in the decrypt form using fuzzy method and semantic search. Finally user can retrieve the data from the server and access our data.The existing solutions supports only identical keyword search, semantic search is not supported. In the project we proposed semantic multi-keyword ranked search system with verifiable outsourced decryption. To improve search efficiency this system includes semantic search by using fuzzy search.

Keywords-*cloud computing based semantic keyword search*

*****

I. INTRODUCTION

1.1Cloud Computing

Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services), which can be rapidly provisioned and released with minimal management effort. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in either privately owned, or third-party data centers that may be located far from the user–ranging in distance from across a city to across the world. Cloud computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility (like the electricity grid) over an electricity network.Advocates claim that cloud computing allows companies to avoid up-front infrastructure costs (e.g., purchasing servers). As well, it enables organizations to focus on their core businesses instead of spending time and money on computer infrastructure. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables Information technology (IT) teams to more rapidly adjust resources to meet fluctuating and unpredictable business demand. Cloud providers typically use a "pay as you go" model. This will lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model

1.2 Cloud computing framework:

In such a frame work, the individual can data owner store her data on the cloud server, namely data outsourcing, and then make the cloud data open for only private access

through the cloud server. This is only used for private access. This represents a more scalabe low cost and stable way for private data access because of the scalability and high efficiency of cloud servers, and therefore is favourable to small enterprises.

II. SYSTEM MODELS

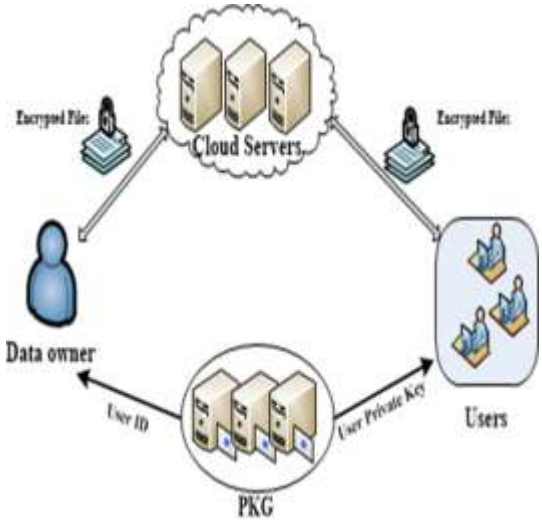


Figure 1. An example of system model

Data owner: To protect the data privacy, the data owner encrypts the original data through symmetric encryption. To improve thesearch efficiency, the data owner generates some keywords for each outsourced document. The corresponding index is then created according to the keywords and a secret key. After that, the data owner sends the encrypted documents and the corresponding indexes to the cloud, and sends the symmetric key and secret key to search users.

Cloud server: The cloud server is an intermediate entity which stores the encrypted documents andcorresponding indexes that are received from the data owner, and provides data access and search services to search users. When a search user sends a keyword trapdoor to the cloud server, it wouldreturn a collection of matching documents based oncertain operations.

Search user:A search user access our outsourced data following the two steps. First, the search user receives both the secret key[a] and symmetric key[b] from the data owner. Second, according to the search keywords, the search user uses the secret key to generate trapdoor(search) and sends it to the cloud server to decrypt our data using symmetric key.

III. SECURITY ANALYSIS

In this paper, we analyze the main security properties of the proposed schemes. In particular, our analysis focuses on how the proposed schemes can achieve confidentially of documents, privacy protection of index and trapdoor, and unlinkability of trapdoor. Other security features are not the focus of our concern. The confidentiality of documents can achieved by encrypted cloud data using ECC algorithm. The privacy protection of index building and trapdoor are used in the security purposes. The secret key are split into two parts. These keys are respectively encrypt the cipher text data. Therefore the index building and trapdoor can be achieved. If the trapdoor generation function is deterministic cloud server can find out the relationship between the same single keyword or multi keyword, then the data can be decrypted. Therefore the trapdoor was a strong unlinkability of trapdoor is a strong thread model.

Related work

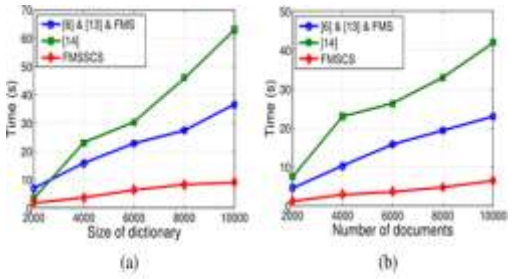
There are mainly two types of searchable encryption in literature, Searchable Secret-key Encryption (SSE) and Searchable Symmetric Encryption (SSE). The previous paper represented a single key word search over encrypted data.This data scheme using public key searchable encryption method. Then he was used Jaccard distance algorithm. But we are using a multiple keyword search on private key. Because security purpose is higher than the public keyword search. Private keyword search have a higher efficiency and scalability;better than the public keyword search. Private key word search using ECC algorithm to encrypt our data to be accessed. Public keyword search method retrieve some irrelevant documents from the cloud data storage. This method cannot support mapping operations. In this paper overcome that our process. We are propose our process at multi data owner scheme can be implemented in the cloud data storage. And it was occurs from the cloud data can be implemented in the public key into two parts at the same time of data downloading. In this paper using a KNN algorithm(K nearest neighbour) using to convert a plain text to cipher text. The search user using to generate a Trapdoor method.

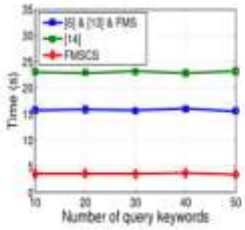
IV. IMPLEMENTATION

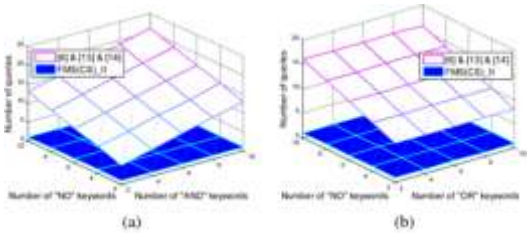
In this paper construct a cloud frame work for data owner and data user. The user generate a multiple key word search on a cloud storage to the data server. The user uploading a plain text file. Then using a two keys to encrypt and decrypt the file. The searchable key words are forma index table in the cloud storage. This index table was very useful in the search in the relevant data on the cloud storage. The data user search the multiple keywords are formed by the random order. Finally the outsourcable data verified by the trapdoor method.

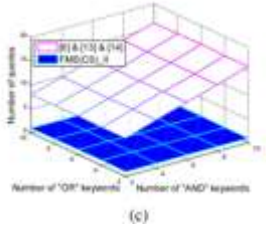
V. PERFORMANCE EVALUATION

In this paper, we evaluate the performance of the proposed schemes using the simulations and we are using the FMS –I and FMS-II are using in the algorithm. The KNN algorithm was mainly used on the performance evolution. The KNN computation scheme was only mainly used for the the multi keyword search. Trapdoor and index building are generate the dictionaries ranking order. The cloud server preserves the encrypted the cloud data and construct the index building and trapdoor generating. These schemes are mainly used for the retrieve the data from the cloud data storage. This KNN algorithm encrypt the plain text to cipher text. The search user and the cloud server are communicate with each other. The data owner needs to cloud server to interact with the data user.









VI. CONCLUSION .

In this project, we tackled the challenging multi-keyword fuzzy search problem over the encrypted data. We proposed and integrated several innovative designs to solve the multiple keywords search and the fuzzy search problems simultaneously with high efficiency. In this approach of leveraging functions to construct the file index is novel and provides an efficient solution to the secure fuzzy search of multiple keywords. In addition, the fuzzy search is adopted to capture the similarity between the keywords and the secure inner product computation is used to calculate the similarity score so as to enable result ranking. We proposed a basic scheme as well as an improved scheme in order to meet different security requirements. And to provide semantic scheme to extract relevant results over encrypted cloud data. We proposed a concrete ABE scheme with verifiable outsourced decryption using a website for an IT firm to store and access documents and thereby proved that it is secure and verifiable. This scheme proved to be more efficient than ABE and ABE with outsourced decryption in every aspect. This intermediate cipher text can be transformed into plaintext by proxy server. This process incurs a small computational overhead. Security of an ABE system with outsourced decryption ensures that an adversary (including a malicious proxy) will not be able to learn anything about the encrypted message; however, it does not guarantee the correctness of the transformation done by the cloud. We also consider a new requirement of ABE with outsourced decryption: verifiability. Thorough theoretical security analysis and experimental evaluation using real-world dataset were carried out to demonstrate the suitability of our proposed scheme for the practice usage.Finally we are implement multi keyword search on cloud frame work. The main advantage of this paper retrieve large relevant data documents on searchable keyword on user. Then easy to analyse the relationship between the multi keyword search.

REFERENCES

[1] H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng, “An smdpbased service model for interdomain resource allocation in mobile cloud networks,” IEEE Trans. Veh. Technol., vol. 61, no. 5, pp. 2222–2232, Jun. 2012.

[2] M. M. Mahmoud and X. Shen, “A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks,” IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 10, pp. 1805–1818, Oct. 2012.

[3] Q. Shen, X. Liang, X. Shen, X. Lin, and H. Luo, “Exploiting geodistributed clouds for e-health monitoring system with minimum service delay and privacy preservation,” IEEE J. Biomed. Health Inform., vol. 18, no. 2, pp. 430–439, Mar. 2014.

[4] H. Li, Y. Dai, L. Tian, and H. Yang, “Identity-based authentication for cloud computing,” in Cloud Computing, Springer, 2009, pp. 157–166.

[5] T. Jung, X. Mao, X. Li, S.-J. Tang, W. Gong, and L. Zhang, “Privacy-preserving data aggregation without secure channel: Multivariate polynomial evaluation,” in Proc. IEEE INFOCOM, 2013, pp. 2634–2642.

[6] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted cloud data,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 222–233, Jan. 2014.