EMAIL SERVER MISBEHAVIOR DETECTION

Gladys.M[1], Hemasri.E[2], Indumathi.B[3], Jayasri.A[4], SELVA KUMAR.A[5]

B.E, (Computer Science and Engineering, T.J.S Engineering College, Tamilnadu, India.

ABSTRACT

With the advent of cloud computing, more and more people tend to outsource their data to the cloud. As a fundamental data utilization, secure keyword search over encrypted cloud data has attracted the interest of many researchers recently. However, most of existing researches are based on an ideal assumption that the cloud server is “curious but honest”, where the search results are not verified. In this paper, we consider a more challenging model, where the cloud server would probably behave dishonestly. Based on this model, we explore the problem of result verification for the secure ranked keyword search. Different from previous data verification schemes, we propose a novel deterrent-based scheme. With our carefully devised verification data, the cloud server cannot know which data owners, or how many data owners exchange anchor data which will be used for verifying the cloud server’s misbehavior. With our systematically designed verification construction, the cloud server cannot know which data owners’ data are embedded in the verification data buffer, or how many data owners’ verification data are actually used for verification. All the cloud server knows is that, once he behaves dishonestly, he would be discovered with a high probability, and punished seriously once discovered. Furthermore, we propose to optimize the value of parameters used in the construction of the secret verification data buffer. Finally, with thorough analysis and extensive experiments, we confirm the efficacy and efficiency of our proposed schemes.

Keyword: - *Cloud Computing, Internet Protocol, JAVA, J2EE, JAVA Servlets, Modules, Testing, Use Case Diagrams, Net Beans, etc…*

1. INTRODUCTION

The requirements specification is a technical specification of requirements for the software products. It is the first step in the requirements analysis process .It lists the requirements of a particular software system including functional, performance and security requirements. The requirements also provide usage scenarios from a user, an operational and an administrative perspective. The purpose of software requirements specification is to provide a detailed overview of the software project, its parameters and goals. This describes the project target audience and its user interface, hardware and software requirements. It defines how the client, team and audience see the project and its functionality. Although cloud computing brings a lot of benefits, for privacy concerns, individuals and enterprise users are reluctant to outsource their sensitive data, including private photos, personal health records, and commercial confidential documents, to the cloud. Because once sensitive data are outsourced to a remote cloud, the corresponding data owner directly loses control of these data. The Apple’s iCloud leakage of celebrity photo in 2014 [3] has furthered our concern regarding the cloud’s data security. Encryption on sensitive data before out-sourcing is an alternative way to preserve data privacy against adversaries. However, data encryption becomes an obstacle to the utilization of traditional applications, e.g., plaintext based keyword search.

1.1 Existing System

- Secure keyword search over encrypted data are based on the ideal assumption that the cloud server is “curious but honest”. Unfortunately,in practical applications, the cloud server may be compromised and behave dishonestly.

- Fuzzy keyword search over encrypted cloud data, respectively.
- Privacy preserving similarity search mechanism.
- To support secure searches in the system where multiple data owners are involved, Secure attribute-based keyword search schemes is proposed.

1.2 Objective

- The ranked keyword system used for exchanging data securely.
- This scheme can be integrated to the ranked keyword search result verification.
- Providing the data owners and users optimal security while accessing and storing their data on the cloud server.

1.3 Contribution

Our aim is to detect of the data has been interfered with and can alert the users and owners at the cloud server is behaving dishonestly by using secured ranked keyword search result verification technique. With the rising use and request of cloud computing an ever-increasing number of individuals will in general tend to re-appropriate their information to the cloud. This not only provides the users with ease of access to their data but also assures them a secure storage space on the cloud. Hence with the potential of billions of people storing tons of volumes of data in the cloud ,the main entity responsible for storage of data attains a vital role in this entire system.

2. LITERATURE SURVEY

The developments in the field of cloud computing increased the efficiency of data owners to deliver information technology services, where various resources such as data and software packages, which are stored in private servers can be retrieved from the internet with the help of various web-based tools and applications instead of having a direct connection with the individual servers. While accessing or sharing information stored in the cloud, the main concern is to enhance the security of data. Different encryption techniques can be used to provide strict privacy requirements. Dual encrypting the data using Advanced Encryption Standard and Homomorphic Encryption scheme enables the data users to ensure the integrity of requested data. Multi-keyword ranked searching enables the data users for efficient retrieval of searched query. Also Identity-Protocol performs the role of user identity verification providing identity tokens to the verified data owners in order to outsource their data in the cloud. Due to the rapid expansion of data, the data owners tend to store their data into the cloud to release the burden of data storage and maintenance[1]. However, as the cloud customers and the cloud server are not in the same trusted domain, our outsourced data may be under the exposure to the risk. Thus, before sent to the cloud, the sensitive data needs to be encrypted to protect for data privacy and combat unsolicited accesses .Unfortunately, the traditional plaintext search methods cannot be directly applied to the encrypted cloud data any more. The traditional information retrieval (IR) has already provided multi keyword ranked search for the data user. In the same way, the cloud server needs provide the data user with the similar function, while protecting data and search privacy. It is meaningful storing it into the cloud server only when data can be easily searched and utilized. With the increasing popularity of cloud computing, huge amount of documents are outsourced to the cloud for reduced management cost and ease of access. Although encryption helps protecting user data confidentiality, it leaves the well-functioning yet practically ecient secure search functions over encrypted data a challenging problem. In this paper, we present a privacy-preserving multi-keyword text search (MTS) scheme with similarity-based ranking to address this problem .To support multi-keyword search and search result ranking, we propose to build the search index based on term frequency and the vector space model with cosinesimilarity measure to achieve higher search result accuracy. To improve the search ecciency, we propose a tree-based index structure and various adaption methods for multi-dimensional (MD) algorithm so that the practical search eciency is much better than that of linear search. To further enhance the search privacy, we propose two secure index schemes to meet the stringent privacy requirements under strong hreatmodels, i.e., known cipher text model and known background model. Finally, we demonstrate the electiveness and eciency of the proposed schemes through extensive experimental evaluation.

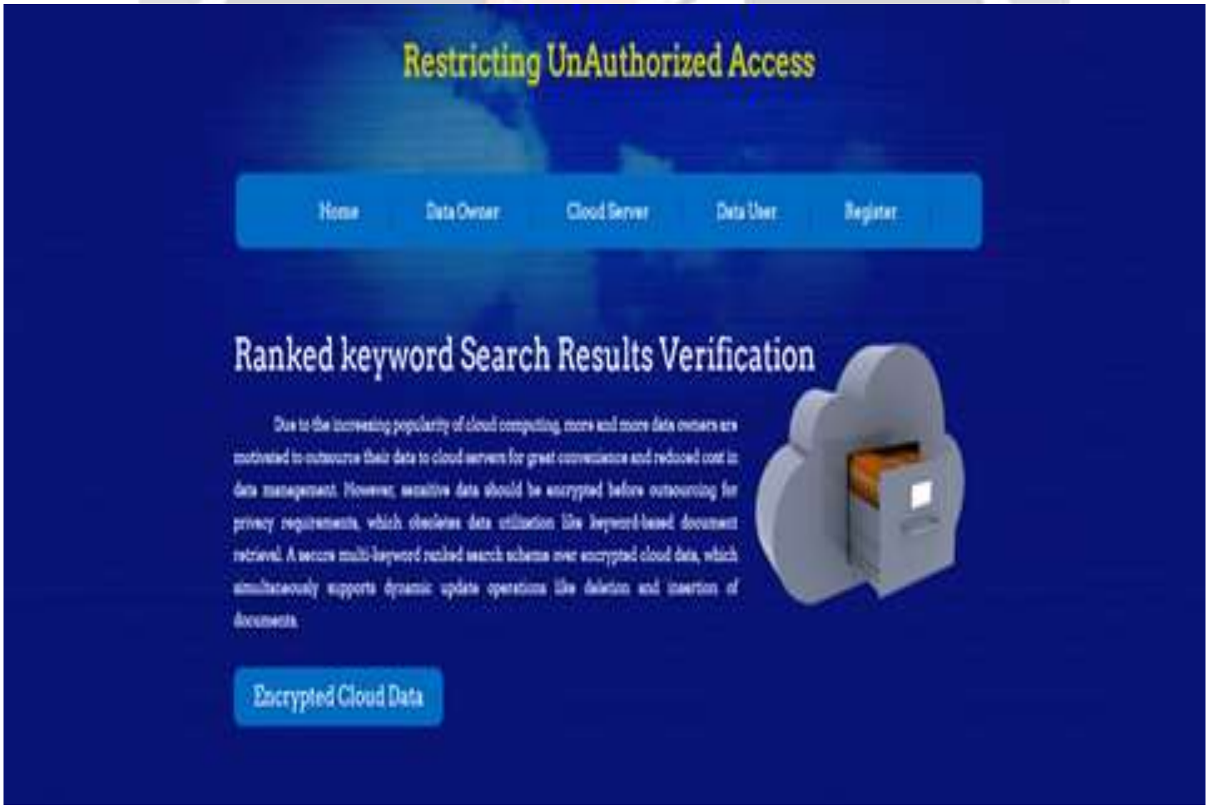
3. PROPOSED SYSTEM

- In this project, multiple data owners are involved so the cloud server would probably behave dishonestly so we explore the problem of result verification for the secure ranked keyword search.
- We propose a novel deterrent-based scheme, with verification data so the cloud server cannot know which data owners or how many data owners exchange anchor data.
- In this project, if any suspicious action is detected, data owners can dynamically update the verification data stored.
- We propose to optimize the value of parameters used in the construction of the secret verification data buffer to confirm the efficacy an deficiency of our schemes.

3.1 Advantages of Proposed System

- The proposed system formalizes the ranked keyword search result verification problem where multiple data owners are involved and it would probably behave dishonestly.
- Our system proposed a novel secure and efficient deterrent based verification scheme for secure ranked keyword search.Our system proposed to optimize the value of parameters used in the construction of verification data buffer.
- The proposed system gives a thorough analysis and conduct extensive performance experiments to show the efficacy and efficiency of our proposed.

4. RESULT

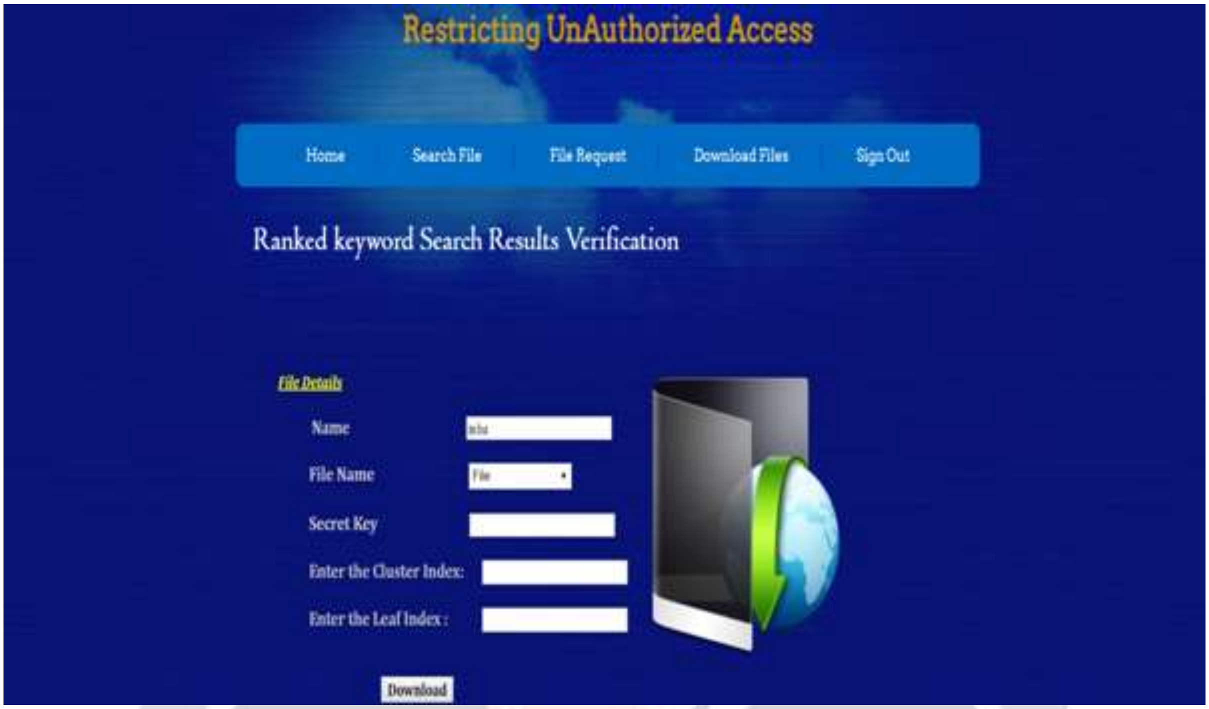


Restricting UnAuthorized Access

Ranked keyword Search Results Verification

Due to the increasing popularity of cloud computing, more and more data owners are motivated to outsource their data to cloud servers for great convenience and reduced cost in data management. However, sensitive data should be encrypted before outsourcing for privacy requirements, which obsoletes data utilization like keyword-based document retrieval. A secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations like deletion and insertion of documents.

Fig.No.1 Screenshot of the Project



Ranked keyword Search Results Verification

File Details

Name [illegible]

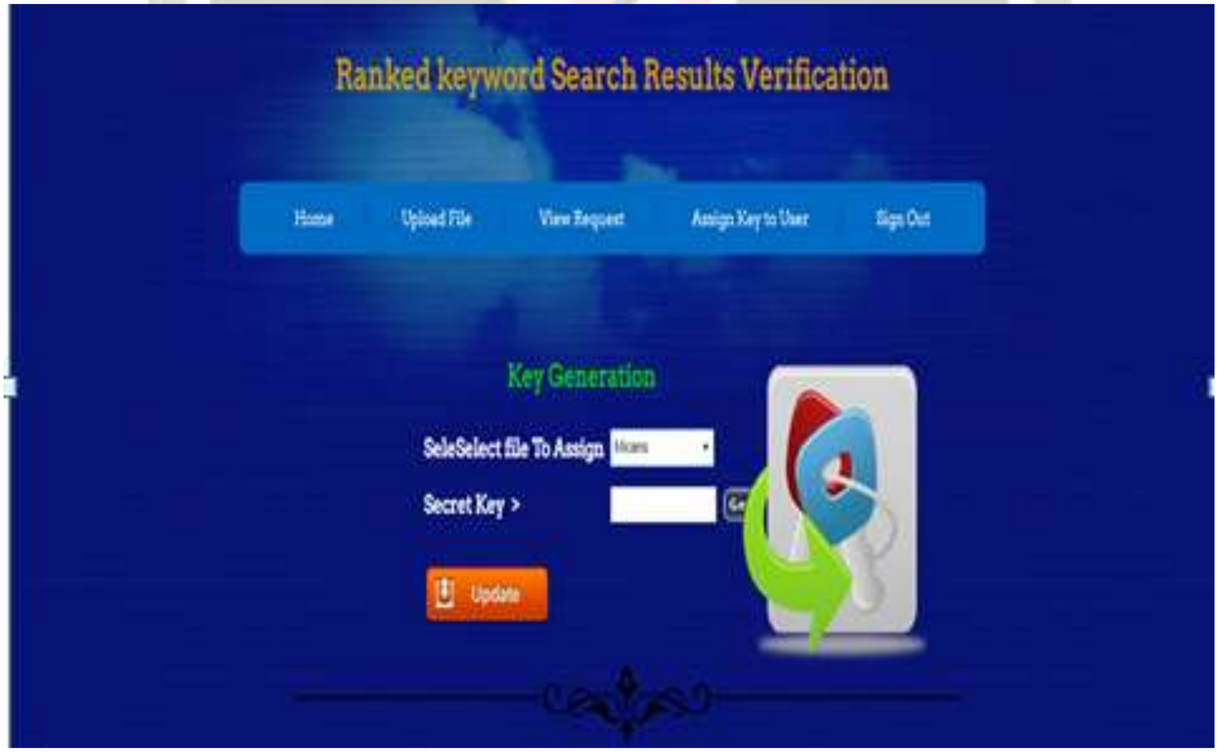
File Name File

Secret Key

Enter the Cluster Index:

Enter the Leaf Index :

Fig.No.2 Screenshot of the Project

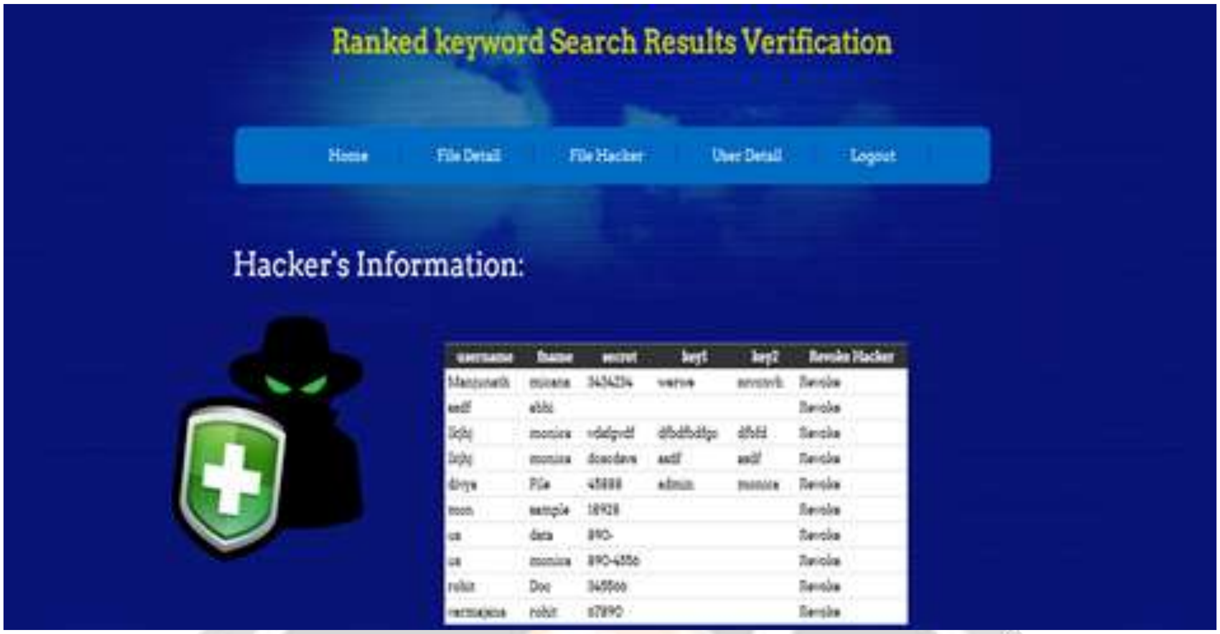


Key Generation

SeleSelect file To Assign [illegible]

Secret Key >

Fig.No.3 Screenshot of the Project



Ranked keyword Search Results Verification

Hacker's Information:

username	fname	secret	key1	key2	Revoke Hacker
Manjunath	monana	3434234	werwe	erwerb	Revoke
asdf	abhi				Revoke
lkjhj	monica	sdafgvdf	dfbdfbdfgs	dfbfd	Revoke
lkjhj	monica	dsacdava	asdf	asdf	Revoke
divya	File	45888	admin	monica	Revoke
moon	sample	18928			Revoke
us	data	890-			Revoke
us	monica	890-4556			Revoke
rohit	Doc	345566			Revoke
vermajena	rohit	s7890			Revoke

Fig.No.4 Screenshot of the Project

5. CONCLUSIONS

Furthermore, our proposed scheme allows the data users to control the communication cost for the verification according to their preferences, which is especially important for the resource limited data users. Finally, with thorough analysis and extensive experiments, we confirm the efficacy and efficiency of our proposed schemes. The purpose of software requirements specifications to provide a detailed overview of the software project, its parameters and goals. This describes the project target audience and its user interface, hardware and software requirements. It defines how the client, team and audience see the project and its functionality.

6. REFERENCES

1. Wei Zhang, *Student Member, IEEE*, and Yaping Lin, *Member, IEEE*, “Catch You if You Misbehave: Ranked Keyword Search Results Verification in Cloud Computing”, IEEE Transactions on Cloud Computing, 2019.

2. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia, "A view of cloud computing", *Commun. ACM*, vol. 53, no. 4, pp. 50-58, 2019.

3. W. Zhang, S. Xiao, Y. Lin, T. Zhou, and S. Zhou, “Secure ranked multi-keyword search for multiple data owners in cloud com- puting,” in Proc. 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN2014). Atlanta, USA: IEEE, 2014, pp. 276–286.

4. Wei Zhang, Yaping Lin, Gu Qi, “Catch You if You Misbehave: Ranked Keyword Search Results Verification in Cloud Computing”, in IEEE Transactions on Cloud Computing, vol. 6, no.1, 2018, pp. 74-86.

5. Qi Chai, Guang Gong, “Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers”, in 2012 IEEE International Conference on Communications (ICC), 2012.

6. Qin Liu, XiaohongNie, Xuhui Liu, Tao Peng, Jie Wu, “Verifiable Ranked Search over dynamic encrypted data in cloud computing”, in 2017 IEEE/ACM 25th International Symposium on Quality of Service (IWQoS), 2017.