Secure And Verifiable Data Sharing For Cloud Using Multi Keyword Searchable Scheme

Vinobha S.V[1], Dr.Manju C Thayammal[2]
[1, 2] Dept of CSE
[1, 2] Ponjesly College of Engineering

Abstract- *In cloud data sharing systems, Searchable Encryption (SE) schemes ensure data confidentiality with retrieving, but it faces several issues in practice. First, most of the previous Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) systems enable users to initiate search requests with a single keyword, which results in many inaccurate results to be returned, thereby wasting computing and bandwidth resources. Second, untrusted cloud servers may return a small portion of incomplete search results to compress communication overhead. Besides, most CP-ABKS schemes only support an unshared multi-owner setting, which incurs a large amount of computational and storage overhead. Furthermore, when the keyword space is a polynomial, most of the previous schemes suffer from offline keyword guessing attacks. To address these issues, we focus on a multi-keyword search scheme which supports the verification of search results without losing efficiency by combining Ciphertext Policy Attribute-Based Encryption (CP-ABE) technology under the shared multi-owner mechanism. We show the security of our scheme, which achieves selective security against offline keyword guessing attacks and guarantees the unforgeability of signatures. The comparison of experimental results illustrates that our scheme is effective and enjoys superior functionalities than the most relevant solutions.*

Keywords- Multi-keyword, attribute-based searchable encryption, verification, shared multi-owner mechanism

I. INTRODUCTION

Cloud computing means on demand delivery of IT resources via the internet with pay-as-you-go pricing. It provides a solution of IT infrastructure in low cost. Actually, Small as well as some large IT companies follows the traditional methods to provide the IT infrastructure. That means for any IT company, we need a Server Room that is the basic need of IT companies. In that server room, there should be a database server, mail server, networking, firewalls, and routers, modem, switches, QPS, configurable system, high net speed and the maintenance engineers. To establish such IT infrastructure, we need to spend lots of money. To overcome all these problems and to reduce the IT infrastructure cost, Cloud Computing comes into existence. The term Cloud refers to a Network or Internet. In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over public and private networks, i.e., WAN, LAN or VPN. Applications such as e-mail, web conferencing, customer relationship management (CRM) execute on cloud.

A New Internet-based computing model has emerged, namely cloud computing which was developed by integrating distributed computing, parallel processing, and grid computing. Today, in a cloud environment, users can conveniently store data and access shared data resources. A large number of companies and individuals share these data to cloud servers for storage. However, despite of the convenience brought by cloud computing, many security issues have been raised. To ensure data security and confidentiality, it is extremely important to improve file privacy.

The traditional method is to store data files on the cloud after being encrypted. Next, Attribute-Based Encryption (ABE) is recognized as an extremely dominant way for achieving fine-grained access control. However, when the data stored on the cloud becomes more, it becomes difficult to retrieve encrypted data. Therefore, how to effectively retrieve encrypted files are critical in practical applications. Searchable encryption (SE) schemes allow users to retrieve encrypted data safely and selectively based on user-specified keywords. Here based on this, a large number of SE solutions based on public key encryption were proposed. Most of these solutions do not realize multi-keyword searches. Because single-keyword search is not powerful enough, it will return many irrelevant search results, resulting in low search efficiency and poor user search experience. Therefore, it is worthwhile to research efficient multi-keyword searchable encryption schemes.

A privacy-preserving Attribute-Based Keyword Search (ABKS) solution was provided. It considers the cloud to be honest but curious. Specifically, the cloud will faithfully obey established conventions, but will also curiously infer valuable information. In practical applications, such assumptions are often insufficient, as cloud servers may output incomplete search results for economic reasons. Therefore, our

scheme considers a semi-honest but curious cloud, and adds a result test to check its integrity. Besides, these SE schemes with fine-grained access control functions are presented, for instance, Ciphertext-Policy ABKS (CP-ABKS) schemes. However, in some applications, the data is owned by multiple data owners rather than one data owner. For example, the patient's electronic medical record is controlled by multiple departments (e.g., outpatient clinics for skin and oral diseases).

In the nonshared multi-owner mechanism, the schemes will incur huge computational and storage costs due to the different data files for each data owner and manager. Therefore, it is more realistic to adopt the multi-owner sharing mechanism, which means that each file is jointly held by multiple data owners. Our research motivation is as follows: The Single-Keyword Search Model is not Accurate Enough. Ciphertext-Policy ABE (CP-ABE) technology is used as a common method for granting access based on the user attributes, obtaining one-to-many encryption and decryption. At the same time, it ensures fine-grained sharing for encrypted data in batches.

However, searchable encryption schemes based on CP-ABE suffer from the following problems: lack of practical multi-keyword search mode; excessive search scope; irrelevant returned results; wasted computational overhead; and poor user search experience. Cloud Servers are Motivated to Return Incomplete Search Results. Most of the existing CP-ABKS schemes set the cloud server to be "honest but curious", and the server can honestly follow the rules to perform search operations. However, in actual situations, cloud servers have the motive to return some false or incomplete search results for a certain benefit. In addition, the non-shared, multi-owner scenario means that each data file has a one-to-one relationship with the data owner, which can incur significant computational and storage costs.

In order to make the ABKS scheme more practical in cloud computing, we are committed to building multi-keyword searchable and verifiable attribute-based encryption on cloud data. It realizes multi-keyword search and the verifiability of search results while ensuring efficiency, and also applicable to shared multi-owner environment to solve the above problems.

Ciphertext-Policy ABE (CP-ABE) technology is used as a common method for granting access based on the user attributes, obtaining one-to-many encryption and decryption. At the same time, it ensures fine-grained sharing for encrypted data in batches. However, searchable encryption schemes based on CP-ABE suffer from the following problems: lack of practical multi-keyword search mode, excessive search scope; irrelevant returned results, wasted computational overhead, and poor user search experience.

II. LITERATURE SURVEY

In recent years, searchable encryption technology and attribute encryption technology have been widely used in cloud storage environments, and attribute-based searchable encryption schemes can both achieve the retrieval of encrypted data and effectively solve the access control problem. Considering that existing attribute-based searchable encryption schemes for cloud storage only support keyword search and do not support attribute revocation, most of the schemes that support attribute revocation only consider the computational overhead of users and ignore the large amount of computational resources consumed by attribute authorization centers when updating keys. In addition, keyword search may lead to partial errors in the returned search results, leading to the wastage of computational and broadband resources. To solve these issues, this paper proposes an attribute-based searchable encryption scheme that supports attribute revocation and is verifiable. To realize fine-grained ciphertext search of encrypted data, support scenarios of dynamic changes of user attributes, and ensure that third-party servers perform the search process reliably and honestly while minimizing computation and storage costs, first, this paper implements attribute revocation with the attribute authorization center by creating a user revocation list and an attribute key revocation list. At the same time, the system updates the attribute key at the time of user search request, which effectively reduces the computational overhead. Second, a third-party auditor is introduced to ensure the correctness of the search results. Finally, the security of this paper is verified by theoretical analysis, and the efficiency and practicality of this paper are verified by comparing it to other schemes through simulation experiments.

Currently, cloud computing has become increasingly popular and thus, many people and institutions choose to put their data into the cloud instead of local environments. Given the massive amount of data and the fidelity of cloud servers, adequate security protection and efficient retrieval mechanisms for stored data have become critical problems. Attribute-based encryption brings the ability of fine-grained access control and can achieve a direct encrypted data search while being combined with searchable encryption algorithms. However, most existing schemes only support single-keyword or provide no ranking searching results, which could be inflexible and inefficient in satisfying the real world's actual needs. We propose a flexible multi-keyword ranked searchable attribute-based scheme using search trees to

overcome the above-mentioned problems, allowing users to combine their fuzzy searching keywords with AND–OR logic gates. Moreover, our enhanced scheme not only improves its privacy protection but also goes a step further to apply a semantic search to boost the flexibility and the searching experience of users. With the proposed index-table method and the tree-based searching algorithm, we proved the efficiency and security of our schemes through a series of analyses and experiments.

Personal health record (PHR) is a medical model in which patients can upload their medical records and defne the access control by themselves. Since the limited local storage and the development of cloud computing, many PHR services have been outsourced to the cloud. In order to ensure the privacy of electronic medical records, patients intend to encrypt their health records before uploading them. However, encrypted PHR can not be accessed directly and not be retrieved by legitimate users. To solve these issues, in this article we propose a new searchable encryption scheme with ciphertext-policy attributes, which achieves fne-grained access control and exact keyword search over encrypted PHRs. Moreover, in our proposed scheme, the receiver can verify the integrity of the search result that the cloud server returns. Finally, we simulate our scheme, and the experiments show that our scheme has high practicability for cloud-based healthcare systems and has high efciency in aspects of keyword search and results verifcation.

A crucial tactic Scalable encryption (SE) enables data safety and functionality in the cloud at one time. The Ciphertext-Policy Attribute-Based Basic Search (CPABKS) utilises CP-ABE, and Ciphertext-Policy Attribute-Based Encryption.plan can accomplish catchphrase based recovery and fine-grained admittance control all the while. Nonetheless, the single characteristic expert intoactive CP-ABKS plans is entrusted with exorbitant client certificate verification and mystery key conveyance. Likewise, this outcomes in a solitary point execution bottleneck in dispersed cloud frameworks. Subsequently, to be able to overcome these restrictions and reduce calculations and capacity issues on asset-restricted cloud-based gadgets frameworks, we provide in this study a secured MABKS, or multi-authority CPABKS framework. The MABKS framework is another feature. is stretched out to help malevolent property authority following and quality update. Our thorough security examination demonstrates the security of the MABKS system across both particular network and particular property models. Our exploratory outcomes utilizing genuine world datasets show the efficiency The efficacy and efficacy of MABKS framework in pragmatic applications.

Searchable encryption permits to upload encrypted documents to a remote honest-but-suspicious server and query that data at the server without the papers having to be decrypted first. With the advent of cloud computing, data owners are encouraged to move their sophisticated data management systems from local sites to commercial public clouds for greater flexibility and cost savings. However, in order to safeguard data privacy, sensitive data must be encrypted before being outsourced, rendering traditional data utilization based on plaintext keyword search outdated. As a result, implementing an encrypted cloud data search service is critical. Given the huge number of data users and documents in the cloud, it is critical for the search service to support multi-keyword queries and result similarity ranking in order to meet the effective data retrieval requirement. In this paper propose the Secured Multikeyword Search over Encrypted Cloud Data, which is based On Quality and Usability of cloud data transmission and storage. Further we used triple DES (Data Encryption Standard) Algorithm of encryption and decryption key for secure authentication process. Here we used different key sizes are used in cryptographic process. Our analysis shows that the suggested approach is secure against adaptive chosen-keyword attacks. This solution is highly efficient and ready to be applied in real-world cloud storage systems, and it also achieves better encryption and decryption execution speed.

III. PROPOSED SYSTEM

In order to make the ABKS scheme more practical in cloud computing, committed to building multi-keyword searchable and verifiable attribute-based encryption on cloud data. It realizes multi-keyword search and the verifiability of search results while ensuring efficiency, and also applicable to shared multi-owner environment. This scheme allows legitimate users to initiate search requests with conjunctive keywords, which can make the search range smaller and quickly locate the desired results, so it will avoid returning useless results and makes users' search experience better. Add a third-party entity and then use a testing mechanism to prevent untrusted cloud servers from outputting incomplete search results. This means that multiple data owners encrypt each data file, which enhances access control, and data users can only decrypt the file after obtaining the permission of multiple data owners. The system includes five entities, namely multiple Data Owners (DOs), Data Users (DUs), Public Cloud Service (PCS), Key Generation Center (KGC) and Public Auditor Server (PAS).

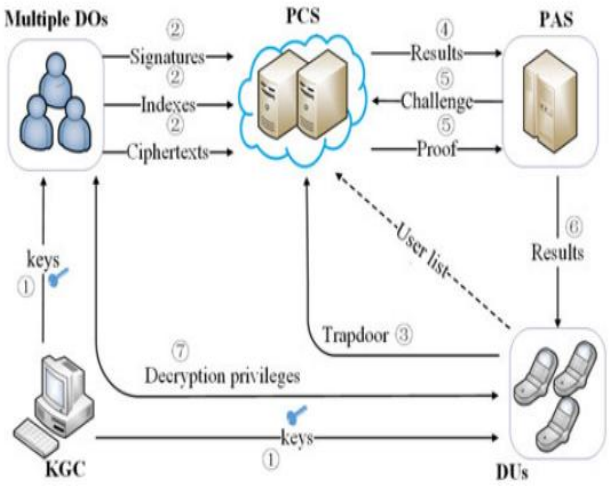

Fig 1. System Architecture

The system includes five entities, namely multiple Data Owners (DOs), Data Users (DUs), Public Cloud Service (PCS), Key Generation Center (KGC) and Public Auditor Server (PAS). First, the KGC is responsible for system initialization and outputting public-private key pairs for users and owners. Then, DOs need to extract multiple keywords from each file and establish indexes, generate file ciphertexts (through traditional symmetric encryption algorithm), generate file encryption key ciphertext, generate file signatures, and then upload them to PCS. The legitimate DU can perform a multi-keyword operation by submitting a search token (or a trapdoor) to PCS. Once the PCS has checked that the search token (or a trapdoor) matches the indexes, it returned the corresponding results to PAS who can test the integrity of results. If it can pass the verification test, then return this result to the DU. Then, DU decrypts them if and only if (s)he has got relevant decryption privileges from multiple Data owner.

Key Generation Center

It performs system initialization and generates the public and private key pairs of DO and DU respectively. A keyword signature is generated for each keyword ciphertext and its associated data ciphertexts. It is used for preventing the cloud from returning incorrect data ciphertexts as the search result.

For each keyword group, one bloom filter is built from its keywords. This allows a data user to check that the searched keyword was indeed not in the keyword group when the cloud returns a null search result, without downloading all keyword ciphertexts from the cloud. A random number is selected and encrypted with the same access control policy as keywords.

The random number masks the bloom filter for preserving keyword privacy. A bloom filter signature is generated for the masked bloom filter and the random number ciphertext for assuring their integrity. A global signature is obtained by signing random number ciphertexts of all groups. It allows a data user to verify the integrity of the random number ciphertexts. A local signature is generated for all keyword ciphertexts within the same keyword group KGj . This signature allows the user to validate the integrity of keyword ciphertexts within the keyword group.

Data Owner

DOs collect files and generate ciphertexts, including file indexes, file ciphertexts, file key ciphertexts and file signatures. It is worth noting that DOs with a shared multi-owner setup use LSSS to generate the file key ciphertexts and use an AND-Gates based access policy to build the index. These final ciphertexts are uploaded to PCS by DO.

A data provider must encrypt it under a DEK (Data Encryption Key) when the data file is sent to the cloud storage. It then establishes an access policy and implements the DEK system. It may also request for deletion of the data file from the cloud storage server.

Data User

A legitimate DU can retrieve the encrypted data according to its own needs, (s)he can issue a search query with conjunctive keywords and generate a search token (or a trapdoor) to PCS. The DU cant decrypt the final results unless (s)he has got relevant privileges from multiple Dos. Every legitimate user will search the data from the system for their benefit. The user creates a search trapdoor to maintain search keyword confidentiality. The consumer then sends his identity to CS and looks for a trapdoor. Without disclosing any keyword search data, the CS can locate the encrypted data including the keywords and do a lot of selective decryption tasks to which the user's decryption load. The user eventually gets the partially decrypted files and then decrypts the partially decrypted files using the partial secret key of his owner.

Public Cloud Service

When PCS receives the search token, PCS tries to match the search trapdoor with established indexes and sends the corresponding results to PAS

Public Auditor Service

To test the accuracy of returned results, PAS and PCS interact in the form of challenge responses. PAS outputs challenge information to PCS, then PCS is required to provide the corresponding proof. Finally, PAS tests whether PCS challenges success. If it succeeds, PAS gives the corresponding results to the DU; otherwise, it gives this DU.

ALGORITHM DESCRIPTION

Optimistic Symmetric Encryption Algorithm

The keys for the RSA algorithm are generated the following way:

1. Choose two different large random prime numbers p and q
2. Calculate n=pq
   - n is the modulus for the public key and the private keys
3. Calculate the totient $\emptyset(n) = (p-1)(q-1)$
4. Choose an integer e such that $1 < e < \emptyset(n)$ and e is co-prime to $\emptyset(n)$ i.e, e and $\emptyset(n)$ share no factors other than 1; $\gcd(e, \emptyset(n)) = 1$
   - e is released as the public key exponent
5. Compute d to satisfy the congruence relation $de \equiv 1\ (mod \emptyset(n))$ i.e, $de = 1 + x\emptyset(n)$ for some integer x
   - d is kept as the private key exponent

The proposed study was to alter the e and n value for a more secure Optimistic Symmetric Encryption Algorithm.

1. Produce Random Large Prime Number p and q.
2. Calculate modulus $n = p * q$.
3. Calculate phi $\emptyset n = (p-1) * (q-1)$
4. Select e with the following condition $\{p > e > \emptyset n, coprime \emptyset n \text{ and } n\}$
5. Calculate $f = (e * 2) + 1$.
6. Select d with the following condition $\{de \bmod n = 1\}$
7. Calculate $g = n - 1$
8. Send Public key (f, g)

The f and g will serve as a new public key which will hide the original e and n value.

9. Send Private key (d, g)

The public key that was sent will be fixed utilizing the modified equation for encryption.

10. Encryption $C = M^{(f-1)/2} \bmod (g+1)$
11. Decryption $D = C^d \bmod (g+1)$

Explanation

In the Key Generation step, the both (private and public) keys are generated to be used in Encryption and decryption process. Generating both keys private and public as shown in below steps:

1. Choose two large prime numbers p and q.
2. Compute modulus number n = p x q.
3. Calculate the Euler function $\emptyset(n) = (p-1)\ x\ (q-1)$.
4. Select an integer number e randomly as a public key. It should satisfy Greater Common Divisor GCD where $(e, \emptyset(n)) = 1, 1 < e < \emptyset(n)$ and coprime with n, $\emptyset n$.
5. Compute the private key d such that de (mod (phi n)) =1

Encryption is the transformation of data into a form that becomes as difficult as possible to read without the appropriate knowledge (a key). In the RSA algorithm the ciphertext is generated by below equation. The Conceptual Framework of Modified RSA Algorithm based on key generation.

$$C = Me\ mod\ n\ (1)$$

A modified key generation of RSA Algorithm will be implemented to improve its security. The method to modify the equation of private key will be utilized which must also concern with the process of encryption and decryption process will be involved. The method to test the two algorithms is to differ the result of RSA factorization calculator.

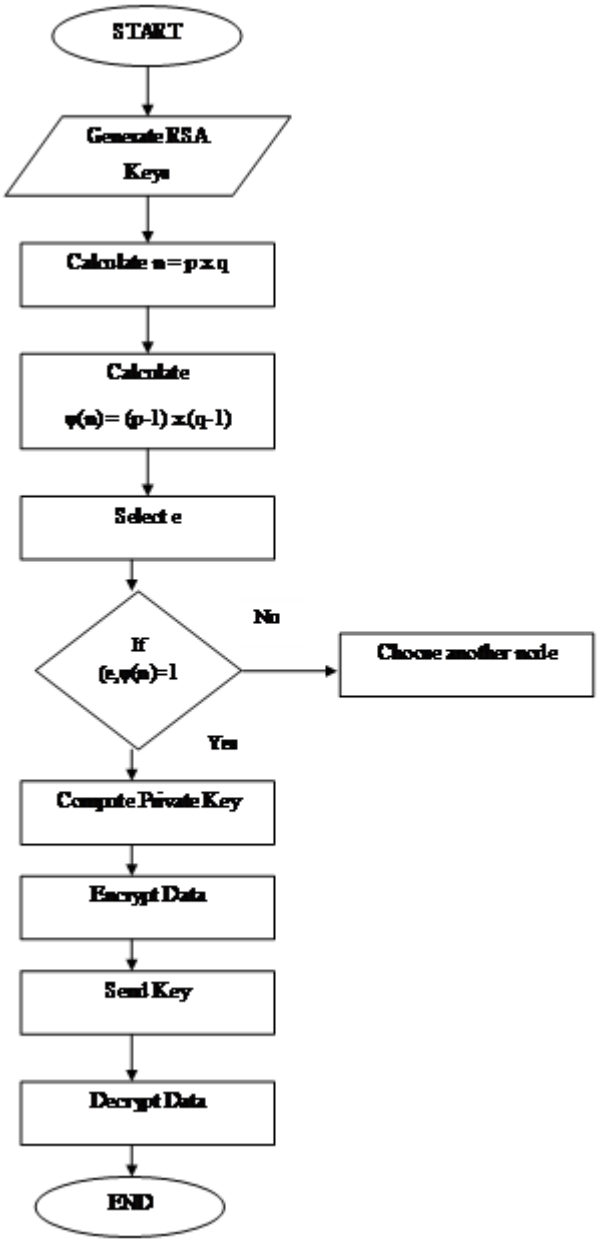

Fig 2. Flowchart

IV. SCREEN SHOTS

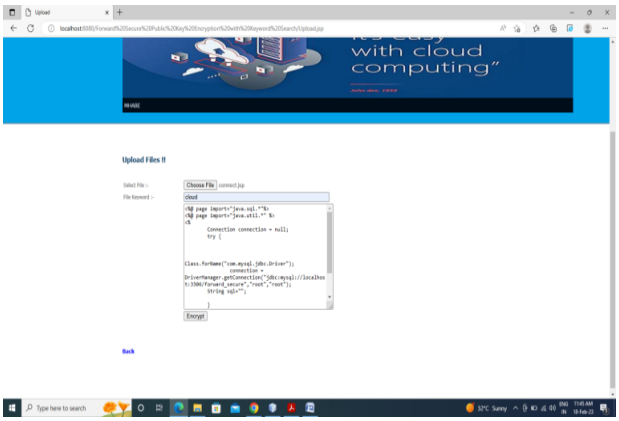

Fig 3. Upload File

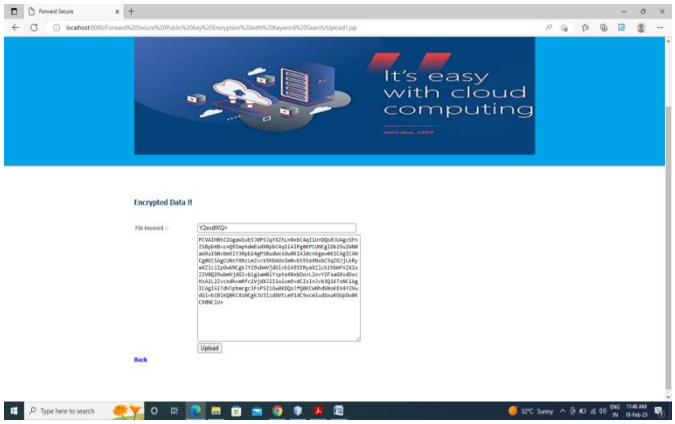

Fig 4.Encrypted Data

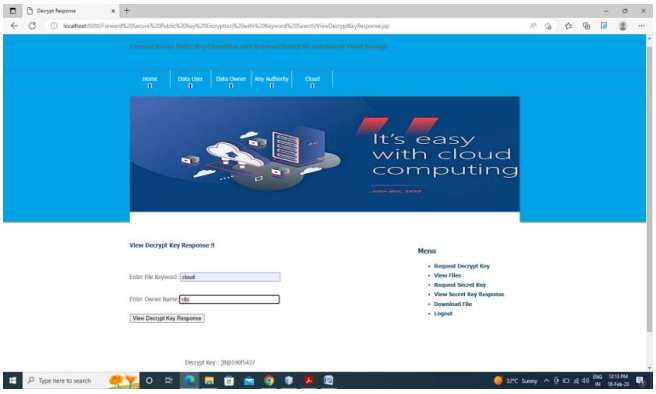

Fig 5. Key Request

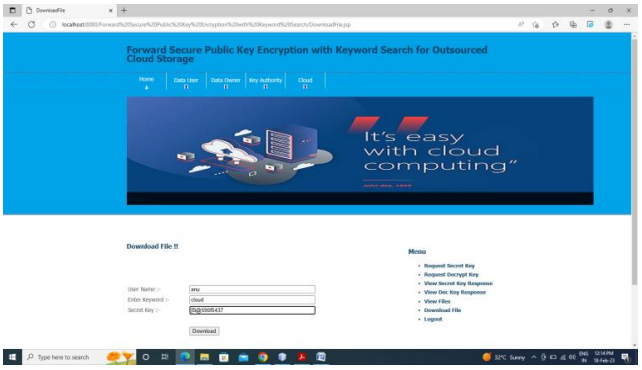

Fig 6. Enter Secret Key

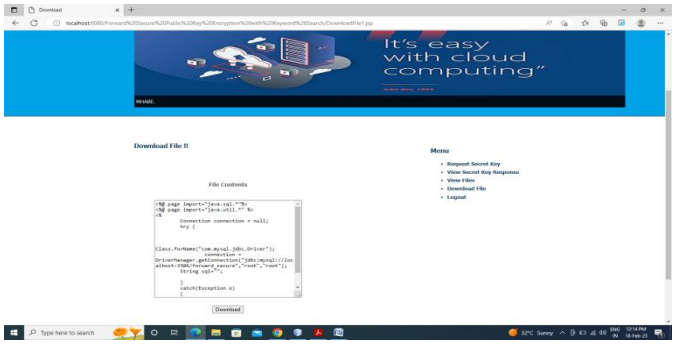

Fig 7. Download File

V. CONCLUSION

Unlike previous searchable encryption schemes, the proposed scheme not only realizes efficient multiple keyword searches, but also uses the third-party entity to ensure the integrity of ciphertext. At the same time, our scheme also supports shared multi-owner mechanism. Our scheme has been proved to be selective security against offline keyword guessing attacks in the general bilinear group model, and guarantees the unforgeability of signatures. Through theory and experiment, it is verified that our scheme is feasible. Besides, with the needs of practical applications, we need to further study and design safer and more efficient search schemes. The future work will focus on building an efficient and flexible index construction so that the ABKS system is capable of supporting various search requests.

REFERENCES

[1] Tao Feng, Sirui Miao, Chunyan Liu and Rong Ma, "Verifiable Keyword Search Encryption Scheme That Supports Revocation of Attributes," Symmetry 2023, 15, 914.

[2] Je-Kuan Lin, Wun-Ting Lin and Ja-Ling Wu., "Flexible and Efficient Multi-Keyword Ranked Searchable Attribute-Based Encryption Schemes," Cryptography 2023, 7, 28.

[3] Yuqin Sun, Lidong Han1, Jingguo Bi, Xiao Tan and Qi Xie., "Verifable attribute-based keyword search scheme over encrypted data for personal health records in cloud," Sun et al. Journal of Cloud Computing (2023) 12:77

[4] Prof. Sreedhar, Sai Sugandiswara Reddy P, "Using Encrypted Cloud Data, Multi-authority Attribute-Based Keyword Search," in Shanlax International Journal of Arts, Science and Humanities, vol. 11, no. S1, 2023, pp. 182–89..

[5] A .Farzana, B. Ananathi, "Privacy Multikeyword Mapping And Search Over Encrypted Cloud Data," 2022 IJRAR January 2022, Volume 9, Issue 1.

[6] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symposium on Security and Privacy (SP'00), 2000, pp. 44–55.

[7] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'04), vol. 3027, 2004, pp. 506–522.

[8] H. Li, D. Liu, Y. Dai, T. H. Luan, and S. Yu, "Personalized search over encrypted data with efficient and secure updates in mobile clouds," IEEE Transactions on Emerging Topics in Computing, vol. 6, no. 1, pp. 97–109, 2018.

[9] J. Ning, J. Xu, K. Liang, F. Zhang, and E.-C. Chang, "Passive attacks against searchable encryption," IEEE Transactions on Information Forensics and Security, vol. 14, no. 3, pp. 789–802, 2019.

[10] X. Zhang, Y. Tang, H. Wang, C. Xu, Y. Miao, and H. Cheng, "Lattice-based proxy-oriented identity-based encryption with keyword search for cloud storage," Information Sciences, vol. PP, pp. 1–15, 2019.