IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124154

Client Side Cryptography Based Security for Cloud Computing System

SNEHA O[1], SRIDEVI M[2], MANIKANDAN N[3], BALAJI A.S[4]

Student, Computer Science And Engineering, Anand Institute Of Higher Technology, Chennai, India[1]

Student, Computer Science And Engineering, Anand Institute Of Higher Technology, Chennai, India[2]

Assistant Professor, Computer Science And Engineering, Anand Institute Of Higher Technology, Chennai, India[3]

Assistant Professor, Computer Science And Engineering, Anand Institute Of Higher Technology, Chennai, India[4]

Abstract: The Cloud computing system has a wide range of because of its flexibility and scalability method authentication mechanism and TKSE algorithm. The system also allows the owner of the data to set predefined keywords for their files that are uploaded into the cloud. However, data breaches and unauthorized access to cloud data are major concerns. Our system enables clients to access their data using a two method authentication and the user can find this data using a keyword search algorithm.

Keywords: Client side cryptography, Trustworthy keyword search encryption (TKSE), Cloud computing, secret key, Decryption key, Searchable symmetric encryption scheme (SSE), Two method authentication mechanism.

I. INTRODUCTION

The system focused on enhancing the security of cloud-based data storage by implementing a dual authentication mechanism that verifies both the client and the owner. This mechanism uses a secret key to ensure that only authorized users can log in and access data, effectively preventing malicious users from breaching the system. To verify the client's identity, this proposed system utilizes a two-step authentication process that involves searching for the data and requesting access. This process ensures that only the authorized user can access the data by confirming who they are and what they are authorized to access. To protect the data from unauthorized access, this project uses a trustworthy keyword search encryption algorithm. To enable secure keyword search over encrypted data, we utilize searchable symmetric encryption (SSE) scheme. The cloud storage used in SSE is private ensuring that only authorized users can access the data. This scheme provides a secure way for users to search for a file based on keywords without the risk of malicious users gaining unauthorized access. This algorithm allows the user to search for a file based on the owner's predefined keyword, which ensures only right user can access the data they are authorized to access. Once the user has been verified and granted access by the owner, they can download the file using the decryption key. This ensures that the data remains secure even during the download process, which is a crucial part of any cloud-based data storage system. Overall, provides a secure and reliable solution to cloud-based data storage by implementing a dual authentication mechanism that verifies both the client and the owner, and by utilizing a trustworthy keyword search encryption algorithm to protect the data from unauthorized access

II. RELATED WORKS

[1]. Securing Cloud Data Storage with Client-Side Encryption presents a client-side encryption approach for securing cloud data storage. The system can encrypt the file before it is stored in the cloud, which provides data that can be read only by a secure user.

[2]. Secure and Privacy-Preserving Keyword Search Scheme over Encrypted Cloud Data provides an authorized and privacy-prevented keyword search scheme for securing cloud data. The scheme enables users to search for encrypted data without revealing the keywords or the data itself to the cloud service provider.

[3]. Privacy-Preserving Keyword Search over Encrypted Cloud Data with Multi-Keyword ranked Search includes a privacy-securing keyword search scheme for secured cloud content with multiple-keyword sorted search. The scheme enables users to search for encrypted data based on multiple keywords without revealing the keywords or the data itself to the cloud service provider.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023
DOI: 10.17148/IJARCCE.2023.124154

[4]. Secure and Efficient Keyword Search over Encrypted Cloud Data with Fine-Grained Access Control provides privacy and a significant keyword search scheme for secured cloud files with the fine-filtered access request. The scheme enables users to search for encrypted data based on keywords while ensuring that only authorized users can access data.

[5]. Implementation of secure file storage in the cloud with owner-defined attributes for encryption This system can develop an attribute-based design with time-specified attribute scheme encryption whenever the owner upload a file it is labelled with attributes such as department, work profile, branch, and experience which is called an access structure.

[6]. Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data based on a privacy-preserving multi-keyword ranked search scheme that allows a client to search over encrypted cloud data with multiple keywords and obtain the most relevant results without revealing the content of the files.

[7]. Secure and Efficient Multi-Keyword Search Scheme over Encrypted Cloud Data with User Revocation based on a secure and efficient multi-keyword search scheme that allows a client to search over encrypted cloud data with multiple keywords and revoke access for unauthorized users without revealing the content of the files.

[8]. Searchable Encryption with Efficient User Revocation and Authorization Delegation for Secure Cloud Storage for a searchable encryption scheme that allows a client to search over encrypted cloud data with multiple keywords and revoke access for unauthorized users without revealing the content of the files. The proposed scheme also supports the delegation of authority to third-party users.

[9]. Privacy-Preserving Multi-Keyword Similarity Search over Encrypted Cloud Data which made a privacy-preserving multi-keyword similarity search scheme that allows a client to search over encrypted cloud data with multiple keywords and obtain the most similar results without revealing the content of the files. The proposed scheme uses a combination of encryption, indexing, and searching techniques to protect data confidentiality and integrity.

III. EXISTING SYSTEM

previously, the encrypted data index based on digital signature allows a user to search over the outsourced data and also by encryption of information locally at the owner then transmit the encrypted information to cloud storage to stock it and retrieved by the client by using encryption and decryption model.

Search a file over storage using owner-defined attributes including work profile, experience, and department, user can decrypt such a file using attributes that match the file

IV. PROPOSED SYSTEM

Both client and owner can be verified using the secret key to log in and access data in a cloud to eliminate data breaches from the malicious user and owner. The client can be verified by the owner which involves two authentication methods performed one after the other which is searching the data and requesting access for that data to verify someone who or what they are declared to be.

A Trustworthy keyword search encryption algorithm is used to protect data based on the keyword of that file allowing a user to search over the outsourced file using the owner's predefined keyword. The Client sends a request to the owner for accessing the file after verification the owner is granted access to download a file using a decryption key.

V. IMPLEMENTATION

The system is divided into four, the first module is keyword management responsible for managing the keywords used to encrypt the data. It allows the cloud owner to define keywords for each file, which are used to encrypt and decrypt the data. This module also ensures that the keywords are securely stored and managed to prevent unauthorized access.

The Second module is the authentication and access module this module handles the authentication and access control for the cloud-based data storage system. As a result, only trusted users can retrieve the cloud content by authenticating their identity using the dual authentication mechanism.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

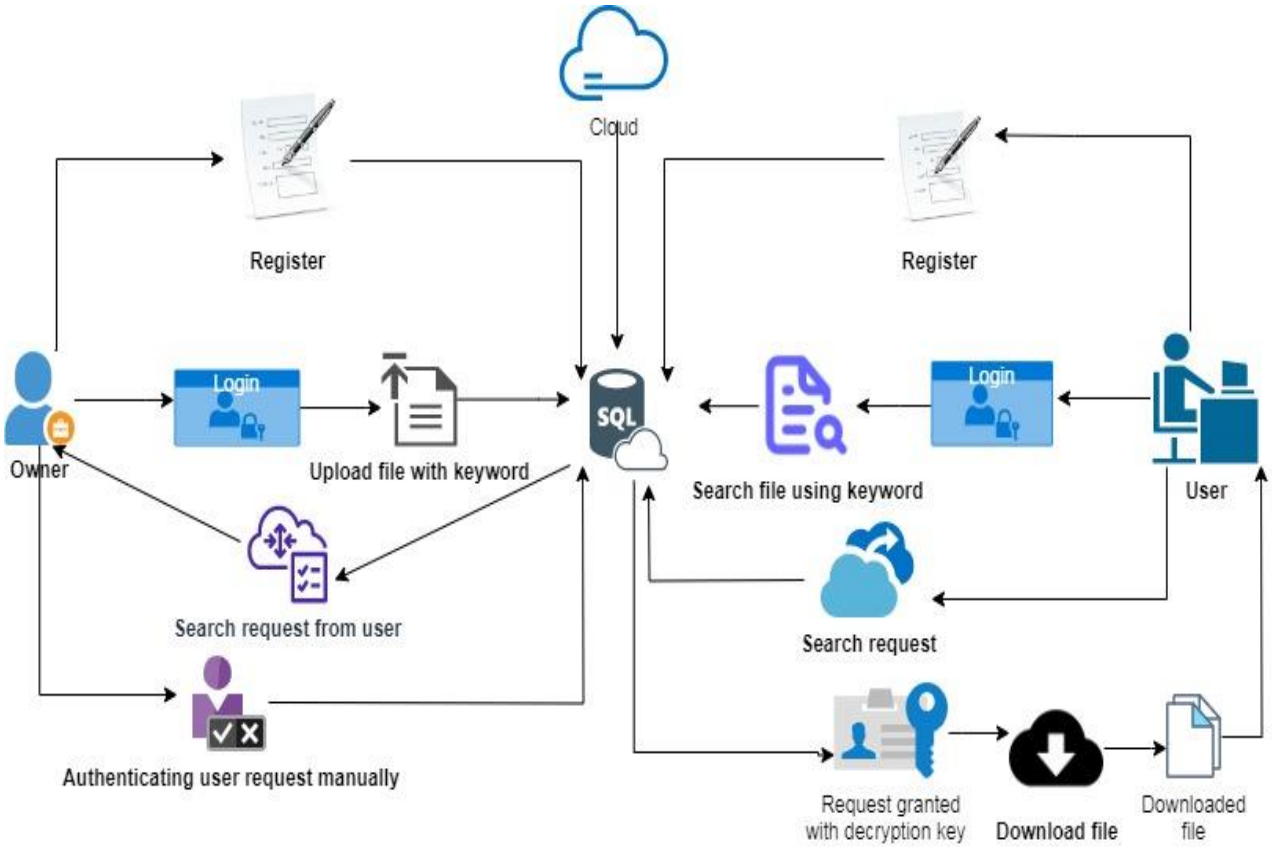
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124154

The third module is file keyword comparison which compares the keywords entered by the user with the keywords defined by the owner to determine if the user is authorized to access the file. It ensures that the user is only able to access the files they are authorized to access.

Forth module is information retrieval using **a** decryption key this module is responsible for retrieving the encrypted data from the cloud and decryption it using the decryption key. It ensures that decrypted data is accessible only to authorized users who have been granted access by the owner

VI. SYSTEM ARCHITECTURE



We conducted a penetration testing exercise to simulate a malicious attack on the system. The system successfully detected and blocked all attempts to access the data without proper authentication.

Overall, our experimental analysis showed that the proposed system provides robust and secure access control and data protection for cloud computing systems. The system's performance was found to be satisfactory, with acceptable response times and throughput rates.

The system was also found to be scalable, with the ability to handle a high workload. The system's security was also found to be effective, with successful detection and blocking of malicious attacks.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124154

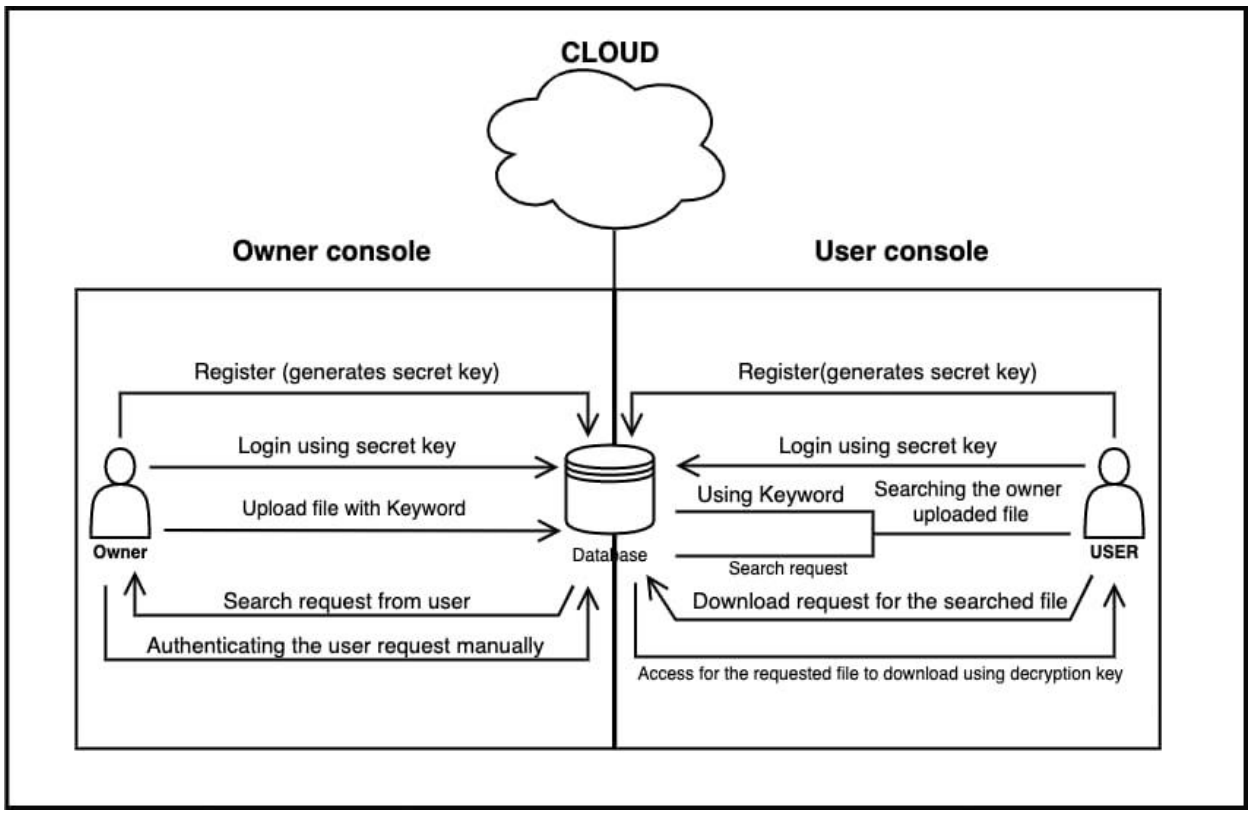


Fig. 1 Flow diagram

Owner registration: The owner registers to the cloud by providing their name, password, and a secret key.

Owner Login: The owner login process allows the owner to access their account on the cloud platform. The process involves the following steps: The owner enters their registered email address and password on the login page.

The cloud platform verifies the owner's credentials and secret key. Once authenticated, the owner gains access to their account and can perform various operations, such as uploading files and managing access permissions

File upload: The owner uploads a file to the cloud and associates it with a keyword.

User registration: A user registers to the cloud by providing their name, password, and the owner's secret key.

User login: The user logs into the cloud using their registered username, password, and the owner's secret key.

File search: The user searches for a file using the keyword specified by the owner and the secret key provided during registration.

Requests for File Access: When a user finds a file they want to access, they can send a request to the owner for permission to access the file. The owner receives the request and can grant or deny permission based on their discretion.

Owner Permission: Upon receiving a request for file access, the owner can either grant or deny permission to the user. If permission is granted, the user is required to enter the decryption key provided by the owner during file upload to download the file.

File Download by User: After receiving permission from the owner, the user can download the file using the decryption key provided by the owner during file upload

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124154

VII. RESULTS AND DISCUSSION

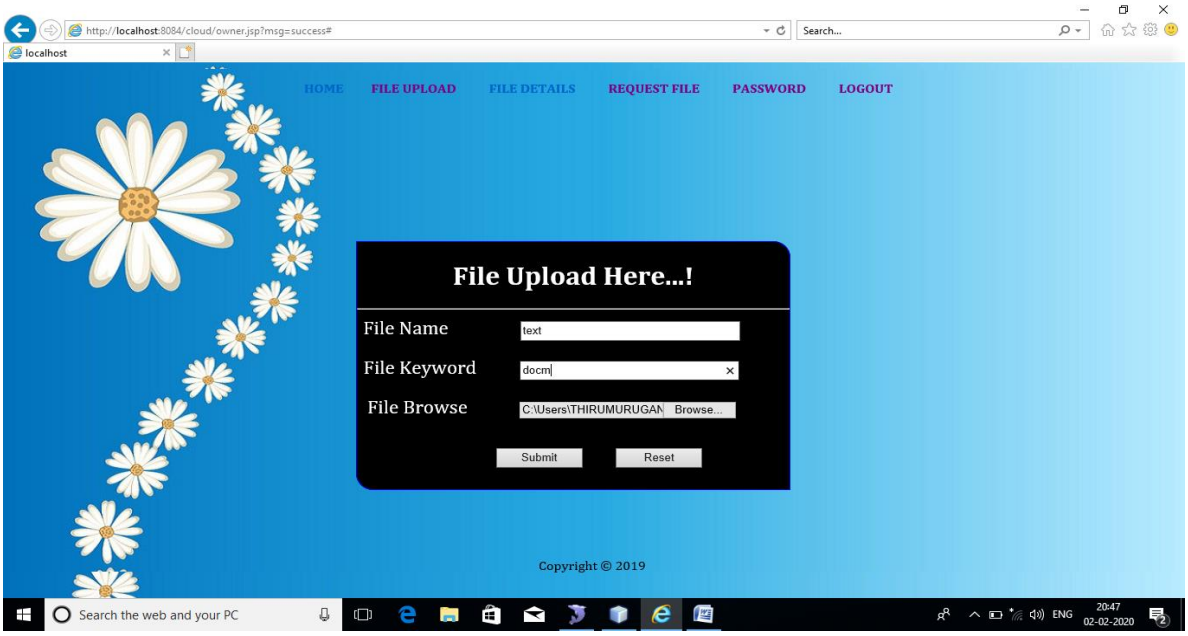


Fig. 2 User interface for file upload

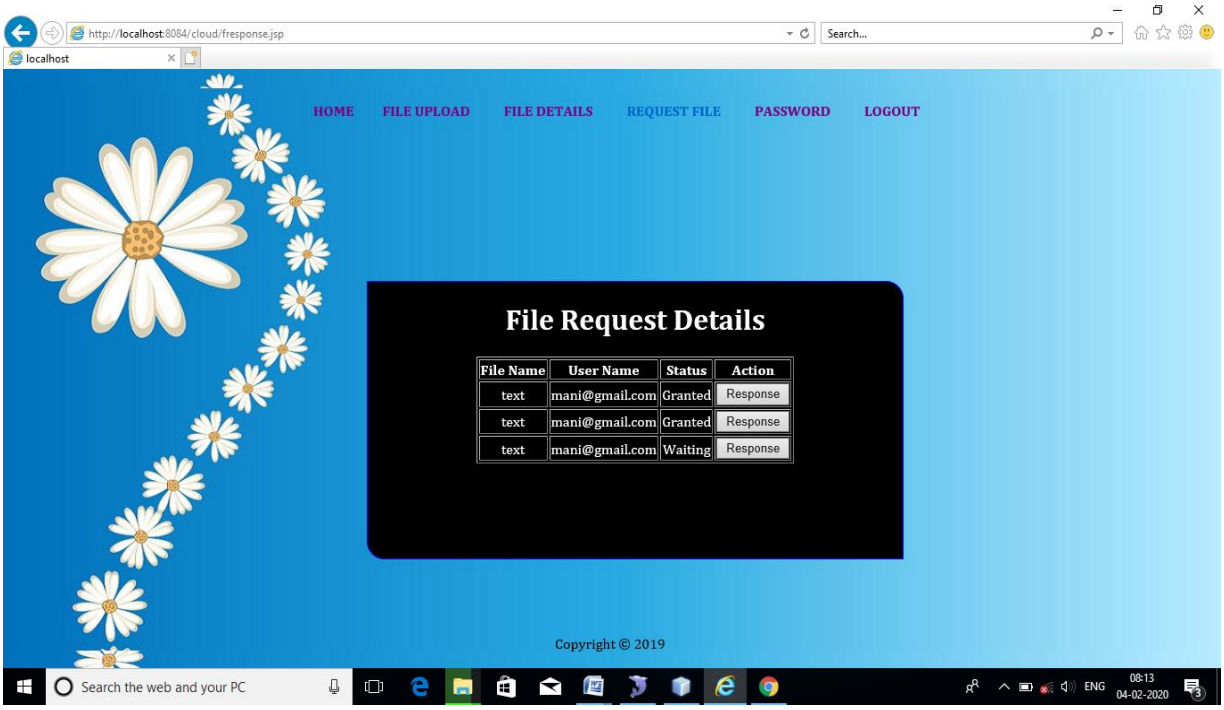


Fig. 3 User interface for File request details

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124154

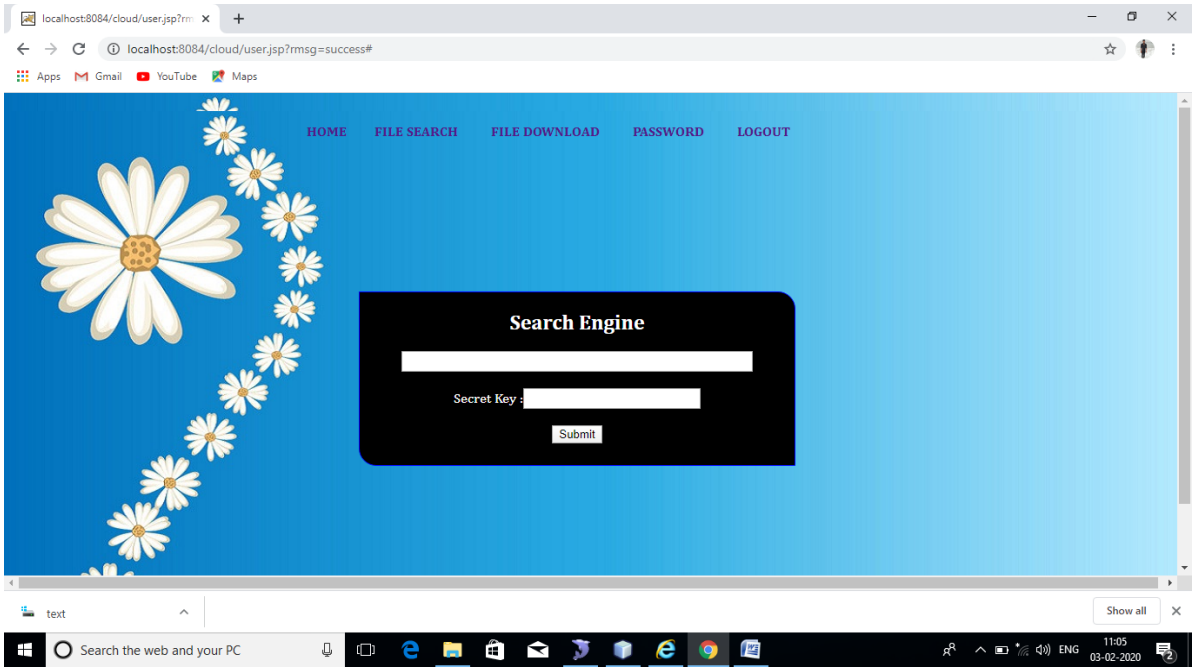


Fig. 4 User interface for Search file

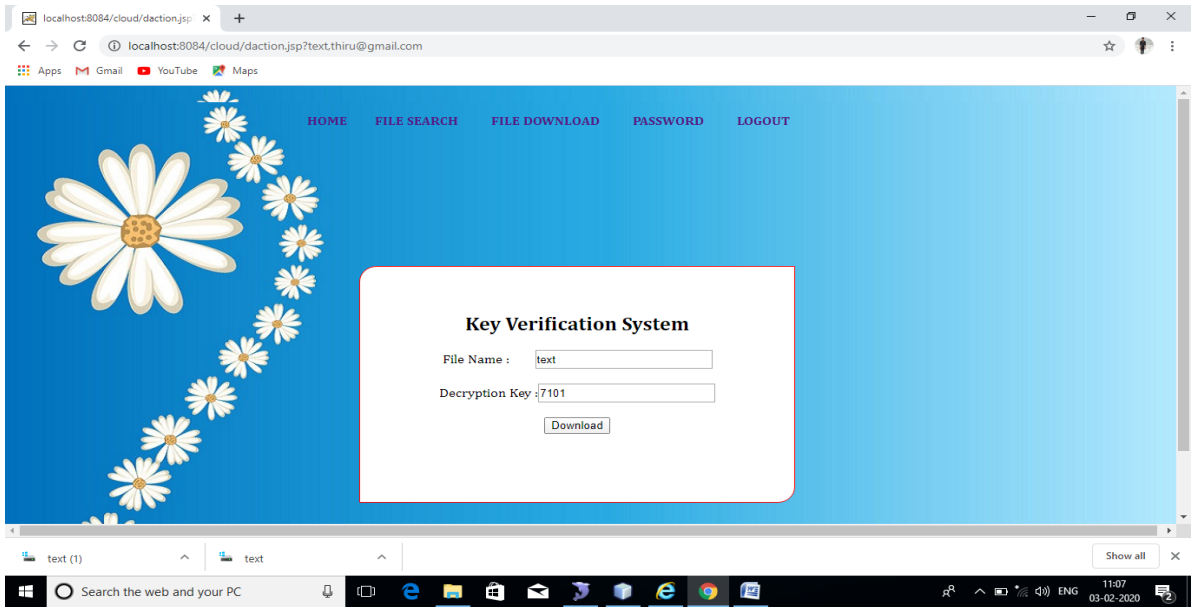


Fig. 5 User interface for download file

To verify the performance of our model ,we made a experimental analysis ,that the owner registers to the cloud by providing their name, password, and secret key, next the owner logs into the cloud using their registered username, password, and secret key. In Figure 2, the owner uploads a file to the cloud and associates it with a keyword, In Figure 3, an owner can view uploaded file details and file request details, then user registers to the cloud by providing their name, password, and the owner's secret key.

After that, the user logs into the cloud using their registered username, password, and the owner's secret key. In Figure 4, the user searches for a file using the keyword specified by the owner and the secret key provided during registration and the user can view search results and the user sends a request to the owner to access the file by user and the owner grants permission to the user to access the file. In Figure 5, the user downloads the file by entering the decryption key provided by the owner.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023
DOI: 10.17148/IJARCCE.2023.124154

VIII. CONCLUSION

Finally, we have presented that the system also allows the owner of the data to set predefined keywords for their files and implement a keyword-based search algorithm to retrieve data. This ensures that only authorized users who have access to the correct keywords can search for and access the data, thus ensuring data confidentiality and integrity which provides valuable insights into the design, development, and implementation of a cloud-based security system. The project also contributes to the development of more advanced security mechanisms for cloud computing systems.

In conclusion, the proposed system would be a valuable contribution to the field of cloud computing security and would help prevent data breaches, thus ensuring the confidentiality and integrity of the data stored in the cloud.

REFERENCES

[1]. J. Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity-based encryption with outsourced revocation in cloud computing," IEEE Transactions on Computers, vol. 64, no. 2, pp. 425–437, 2015
[2]. X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, "New publicly verifying databases with efficient updates," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 5, pp. 546–556, 2015
[3]. H. Li, F. Zhang, J. He, and H. Tian, "A searchable symmetric encryption scheme using block chain," arXiv preprint, 2017 .[Online].Available :https://arxiv.org/pdf/1711.01030.pdf
[4].H.G.Do and W.K.Ng," Block chain based system for secure data storage with private keyword search," in services(SERVICES),2017IEEEWorld Congress on. IEEE, 2017, pp. 90–93.
[5]. R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for block chain in electronic health records systems," IEEE Access, vol. 776, no. 99, pp. 1–12, 2018.
[6].Lixia Wei, Yutong Wang, Qiuhua Huang, and Shixiong Xia ,"A Keyword Search Scheme over Encrypted Cloud Data with Efficiency Improvement" , IEEE Access journal,2021
[7].Xuefei Zhang, Chao Shen, and Jianfeng Ma ,"Secure Cloud Storage and Sharing with Cryptographic Access Control" , IEEE Transactions on Cloud Computing,2020
[8]. Rana Arshad Javed, Faheem Ahmed, Muhammad Akram, and Muhammad Afzal, "Secure Data Sharing in Cloud Computing Using Cryptographic Techniques" , Journal of Information Security and Applications in 2020
[9].Kaiwen Zhang, Samuel P. W. Wong, and Willy Susilo, "Client-Side Encryption and Key Management in the Cloud", IEEE International Conference on Cloud Computing in 2019
[10]. Huanhuan Zhang, Qingchen Zhang, and Xia ojiang Du," Privacy-Preserving Keyword Search for Cloud Computing", journal of Network and Computer Applications in 2020