Securing Cloud Data with Blockchain Based Approach

Dr K Madan Mohan[1], P Nithin Kumar[2], P Raghava Reddy[3] , S Mani Chandh[4]

[1]Associate Professor, Department of CSE, Gurunanak Institute of Technology, Telangana, India.
[2]UG Scholar, Department of CSE, Gurunanak Institute of Technology, Telangana, India.
[3]UG Scholar, Department of CSE, Gurunanak Institute of Technology, Telangana, India.
4UG Scholar, Department of CSE, Gurunanak Institute of Technology, Telangana, India.

---***---

Abstract - The use of encryption is essential to protect sensitive data, but it often poses challenges when it comes to locating and retrieving information without decryption. Searchable encryption provides an effective mechanism that achieves secure search over encrypted data. In this paper a new approach to address the fine-grained search and to protect sensitive data, Blockchain Assisted ciphertext policy decentralized attribute-based encryption (BA-CP-DABE) in cloud has been developed. The CP-DABE is employed to manage data access, secure key generation, while the immutability of blockchain ensures the confidentiality of ciphertext. By leveraging searchable encryption, it becomes possible to securely search encrypted data stored on the blockchain. Keywords are encrypted using attribute-based encryption and stored on a remote server, along with the corresponding ciphertext in the blockchain. One of the significant challenges in this approach is the assumptions-based technique i.e., bilinear mapping, which involves keyword ciphertext and trapdoor security. However, through extensive numerical experiments, the system has demonstrated its ability to generate key and trapdoor structures, as well as effectively find keywords within the encrypted data.

Key Words: Searchable Encryption, Attribute-Based Encryption (ABE), Ciphertext-Policy ABE (CP-ABE), Decentralized ABE (DABE)

1. INTRODUCTION

With the rise of cloud storage, ensuring data privacy and searchability over encrypted data has become a major concern. Traditional encryption methods protect data but significantly hinder search efficiency, requiring users to download and decrypt large datasets. To address this, **Searchable Encryption (SE)** enables users to search over encrypted data using specific keywords, reducing bandwidth usage and preserving confidentiality.

However, most SE schemes lack robust access control, especially in multi-user environments. **Attribute-Based Encryption (ABE)** provides fine-grained access by embedding user attributes into encryption keys or policies. Despite its advantages, ABE faces challenges such as attribute revocation, policy privacy, and dynamic authorization.

Recently, **blockchain technology** has emerged as a solution to enhance trust, transparency, and immutability in distributed systems. Combining ABE with blockchain enables secure, auditable, and decentralized data sharing while supporting dynamic policy updates.

In this project, we propose a **novel distributed data-sharing scheme** that integrates blockchain and **Attribute-Based Searchable Encryption (ABSE)**. Our approach supports fine-grained keyword search over encrypted cloud data, enforces dynamic access control based on user attributes, and maintains low computational overhead. Additionally, it ensures policy privacy, supports attribute revocation, and leverages blockchain to guarantee data integrity and secure authorization.

This research contributes a secure and efficient data-sharing framework that enhances privacy, user control, and access flexibility in distributed cloud environments.

2. OBJECTIVE

The emerging distributed and decentralized networks, such as wireless sensor networks (WSN), MANETs, VANETs, smart-grid networks, etc., cannot assume trust in a single entity such as the key generation center (KGC). Hence, trust and power must be distributed to the group members. Considering all the above-stated reasons, we are motivated to design an efficient and secure certificateless cryptography-based decentralized and distributed network setup for shared group data auditing without the need for a trusted central authority and that can mitigate security issues arising from a compromise of KGC as possible in the existing works and enable secure flexible new user admission.

The contributions of this paper are as follows:

1. Our scheme provides secure new user entity admission for shared group data auditing. The new entity can become a full member with all the capabilities or a semi-member with limited capabilities.
2. A user entity can request and compute a private-public key pair associated with the group secret. The private-public key pair will be useful to generate metadata (digital signatures), pairwise symmetric keys, and decrypt messages. The scheme is secure against metadata forgery, and public key replacement attacks. It also prevents the precomputation of integrity proofs. In contrast, many existing schemes suffer from the same.
3. The scheme utilizes the FOG computing capabilities to establish secure broadcast group key agreement and communication among the edge device and the group members.
4. The scheme supports aggregate auditing of shared group data by the data auditor. At the same time, it can also perform aggregate verification of the auditing proofs of the data auditor. Hence, the metadata generation mechanism's aggregate property improves the auditing task's efficiency.

3. BLOCKCHAIN TECHNOLOGY

Definition:

A decentralized, tamper-proof ledger used for secure and transparent record-keeping.

Role in Project:

- **Decentralized Access Control:** Stores access policies on blockchain, removing central authority.
- **Immutable Logging:** Records all access/modification attempts permanently.
- **Smart Contracts:** Automate access enforcement and secure data triggers.
- **Verification:** Data owners can verify policy enforcement without trusting the cloud.

Benefits:

- Trustless security using cryptographic proofs
- Tamper-resistant logs and policies
- Full transparency and auditability
- Secure, collaborative data sharing

Challenges:

- High latency and low throughput
- Operational costs (e.g., gas fees)
- Scalability issues with complex policies

4. CP-DABE (CIPHERTEXT-POLICY DECENTRALIZED ATTRIBUTE-BASED ENCRYPTION)

Definition:

A cryptographic scheme enabling fine-grained access control based on user attributes, without a central authority.

Role in Project:

- **Fine-Grained Control:** Encrypts data with attribute-based policies
- **Decentralized Authorities:** Multiple AAs manage keys, reducing failure risks
- **Dynamic Authorization:** Easily manage user access and revocation
- **Smart Contracts:** Handle authentication and access logging

Architecture:

- **Data Owner:** Encrypts data and posts policy hash on blockchain
- **Attribute Authorities:** Issue attribute keys
- **Users:** Decrypt data if their attributes meet the policy
- **Smart Contracts:** Enforce and track access

Benefits:

- Scalable and secure multi-authority access control
- Supports revocation without re-encryption

- Preserves policy privacy

Challenges:

- Complex key management
- High computation cost
- Risk of attribute collusion by users

5. LITERATURE SURVEY

Blockchain-Based Approaches for Secure Search over Encrypted Data

[1] Z. T. Guan, N. Y. Wang, X. F. Fan, X. Y. Liu, L. F. Wu and S. H. Wan, "Achieving secure search over encrypted data for e-commerce: A blockchain approach," 2021.

Title: Achieving secure search over encrypted data for e-commerce: A blockchain approach
Explanation:
This paper introduces the Consortium Blockchain-based Distributed Secure Search (CBDSS) scheme to enable secure search over encrypted data in e-commerce. It integrates blockchain and searchable encryption to ensure only authorized nodes access the system. A novel endorsement strategy divides and assigns search tasks based on node capacity. Security and performance evaluations confirm the scheme's robustness and reliability over conventional methods.

[2] H. Y. Li, T. Wang, Z. R. Qiao, B. Yang, Y. Y. Gong, J. Y. Wang, et al., "Blockchain-based searchable encryption with efficient result verification and fair payment," 2021.

Title: Blockchain-based searchable encryption with efficient result verification and fair payment
Explanation:
This work addresses verifiability and incentive issues in blockchain-based searchable encryption. By outsourcing result verification to the True Bit network, it mitigates the Verifier's Dilemma, ensuring result accuracy. Additionally, it proposes a fair payment protocol for data owners and users and introduces permission revocation. Experiments on Ethereum smart contracts validate the scheme's practicality and low computational overhead.

[3] J. Li, Y. Y. Huang, Y. Wei, S. Y. Lv, Z. L. Liu, C. Y. Dong, et al., "Searchable symmetric encryption with forward search privacy," 2021.

Title: Searchable symmetric encryption with forward search privacy

Explanation:
The authors propose an advanced notion of forward search privacy to prevent information leakage during search queries on encrypted data. A novel technique called Hidden Pointer Technique (HPT) enables a new SSE scheme named *Khons*, which satisfies forward and forward search privacy. Evaluated on a large-scale Wikipedia dataset, Khons outperforms existing SSE solutions in efficiency and privacy.

[4] X. Q. Liu, G. M. Yang, W. Susilo, J. Tonien, X. M. Liu and J. Shen, "Privacy-preserving multi-keyword searchable encryption for distributed systems," 2021.

Title: Privacy-preserving multi-keyword searchable encryption for distributed systems

Explanation:
This study presents a searchable encryption scheme that supports multi-keyword search in multi-user environments, addressing challenges like search/access pattern leakage and keyword guessing attacks (KGA). A multi-server architecture enhances response time, security, and workload distribution. A novel subset decision mechanism is introduced, enabling broader applicability beyond keyword search. The scheme is both secure and efficient.

[5] K. He, J. Chen, Q. X. Zhou, R. Y. Du and Y. Xiang, "Secure dynamic searchable symmetric encryption with constant client storage cost," 2021.

Title: Secure dynamic searchable symmetric encryption with constant client storage cost

Explanation:
This paper introduces *CLOSE-F* and *CLOSE-FB*, two dynamic SSE schemes based on a two-level fish-bone index chain structure (LoKIC and DIC). They provide forward and backward security with constant storage cost on the client side, overcoming a major limitation of traditional DSSE. Experiments confirm their computational efficiency and minimal client storage requirements.

[6] Q. Y. Song, Z. T. Liu, J. H. Cao, K. Sun, Q. Li and C. Wang, "SAP-SSE: Protecting search patterns and access patterns in searchable symmetric encryption," 2021.

Title: SAP-SSE: Protecting search patterns and access patterns in searchable symmetric encryption
Explanation:
SAP-SSE is a novel SSE framework that concurrently protects access and search patterns using re-encryption techniques and distributed secure indexes. It supports multi-user operations in generic database environments. An index redistribution protocol and configurable security policy further strengthen its adaptability. Formal analysis and experiments confirm its strong privacy guarantees and operational efficiency.

6. PROBLEM STATEMENT

Traditional cloud storage lacks strong privacy and integrity protections. This paper proposes a Privacy-Preserving Searchable Encryption (PPSE) scheme using public and private blockchains and smart contracts to enable secure, verifiable, and access-controlled data search without relying on a central server.

6.1 Existing System

1. SE schemes enable keyword-based search on encrypted data using encrypted indexes and tokens.
2. Early systems were inefficient, especially as data size increased.

6.2 Disadvantages of Existing System

1. Traditional encryption doesn't support search functionality.
2. Low data security.
3. Poor efficiency and practicality.
4. Risk of leaking sensitive data to unauthorized users.

6.3 Proposed System

1. The proposed PPSE scheme integrates blockchain-based smart contracts to handle search queries and enforce access control, ensuring data privacy, correctness, and integrity without central authority.

6.4 Advantages of Proposed System

1. Provides data authentication.
2. Offers strong security against attacks.
3. Ensures high efficiency and practical usability.

7. METHODOLOGY

7.1 MODULES NAMES

This project having the following 5 modules:

1. Data Provider Interface:
2. File Encryption
3. Data Utilizer Module
4. Request To Authenticator
5. File Decryption Technique

7.2 MODULES EXPLANATION

1) DATA PROVIDER INTERFACE

This is the first module of our project. In this the data provider first creates an account by using registration, immediately the application server sends public key when account is created successfully. Only authenticated users can login to the application by using their username and password. The data provider can't possess any rights after login. Data provider will get a secret key after proper login. Data provider supposed to submit those public and secret keys which are provided by the server then only can able to upload data to the application cloud storage.

2) FILE ENCRYPTION

This is the second module of our project. In this the data provider uploads the files which are outsourced securely by using encryption. The encrypted data is known as cipher text which is not readable. The data provider also not able to access the original content directly from the cloud storages once he is uploaded that. He only can able to view the already uploaded file details along with the content of the file but it is visible in cipher text.

3) DATAUTILIZER MODULE

This is the third module of our project. In this the user first create an account as a data utilizer. Then only able to login. After login to the application, If the data utilizer get the permission from the authenticator he can able to search the files which are uploaded by the data provider and access the file content otherwise can get flaws like not requested to authenticator and so on…

4) REQUEST TO AUTHENTICATOR

This is the fourth module of our project. In this the data utilizer's who are not able to access the files which are uploaded by the data provider's perform two steps. First if not send request to the authenticator immediately send request providing username and email-id. Second wait for the authenticator to respond to your request. Then only able to access the files but they are in encrypted format.

5) FILE DECRYPTION TECHNIQUE

This is the fifth module of our project. In this the authenticated data utilizer submit the encrypted file name to server. Which will cross checks and provides the decryption key along with an instant key next can able to collect the blocks of data. Properly submit the decrypt key and instant key then only get the original file.

8. ALGORITHM OR TECHNIQUES:

PPSE Overview: A hybrid encryption scheme leveraging both public and private blockchains for secure, searchable, and privacy-preserving data management.

Blockchain Roles:

- **Public Blockchain:**

a) Open access, ensures transparency and immutability.

b) Uses PoW/PoS for security.

c) Pros: Decentralized, censorship-resistant, irreversible.

- **Private Blockchain:**

a) Access controlled by a single organization.

b) Faster, cheaper, and more secure for sensitive data.

c) Ideal for enterprise use.

Core PPSE Algorithms:

1. **Setup (λ):**

a) DO initializes with security parameter λ, generates key *k*.

b) Creates empty Map and EDB.

c) Uses KC-IDC structure: (keyword *w*, file ID *id*).

2. **Search (k, Map, G, w):**

a) DU requests access; authorization checked.
b) Smart contracts search data:
i.If keyword status = Y → no update since last search.
ii.Else, generate new pointer for updated data.

3. **Addition (k, G, Hash, Map):**

a) DO updates keyword status:

- New key/token if it's a first update after search.

b) Data is encrypted, hashed, and:

i.Encrypted data → public blockchain.

ii.Hash → private blockchain.

c) Map is updated.

4. **Delete (blockNo, db(w), EDB):**

a) DO triggers smart contract via block number.

b) Contract removes encrypted data from public blockchain.

9. DESIGN AND DEVELOPMENT

Design Engineering deals with the various UML [Unified Modelling language] diagrams for the implementation of project. Design is a meaningful engineering representation of a thing that is to be built. Software design is a process through which the requirements are translated into representation of the software. Design is the place where quality is rendered in software engineering. Design is the means to accurately translate customer requirements into finished product.

9.1 SYSTEM ARCHITECTURE

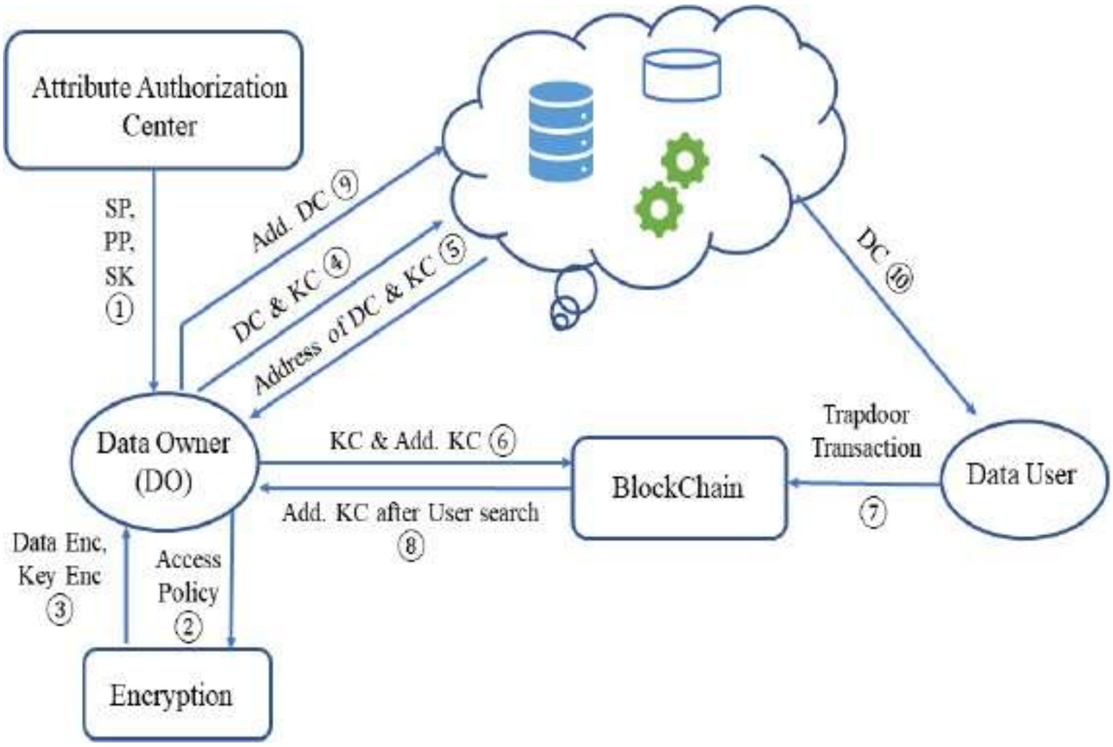


Figure-1: System Architecture

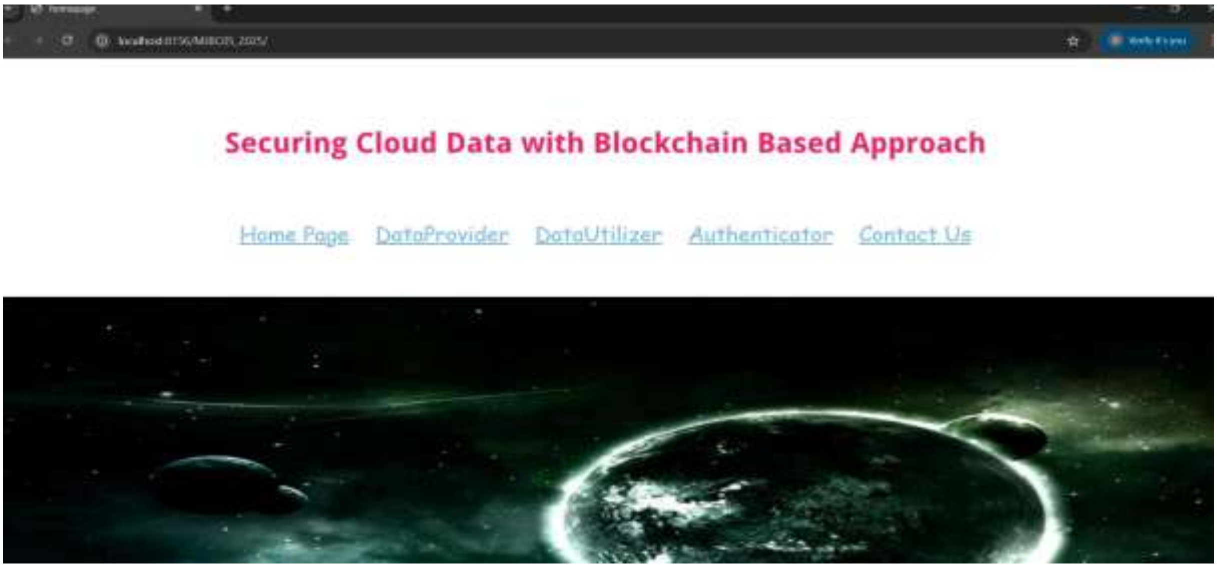
The Privacy-Preserving Searchable Encryption (PPSE) system protects cloud data using blockchain and attribute-based access control. It involves four parts: Attribute Authorization Center, Data Owner (DO), Data User (DU), and cloud storage linked to blockchain.

The process starts with the Authorization Center giving the Data Owner cryptographic keys. The Data Owner sets access rules, encrypts the data and keys, and uploads them to the cloud. The cloud returns the data address, and the DO stores the key info on the blockchain.

When a Data User wants to access data, they send a search request (trapdoor) to the blockchain. The blockchain checks permissions through smart contracts and, if valid, allows access. The user then downloads the encrypted data from the cloud.

This system ensures secure, private, and controlled data access.

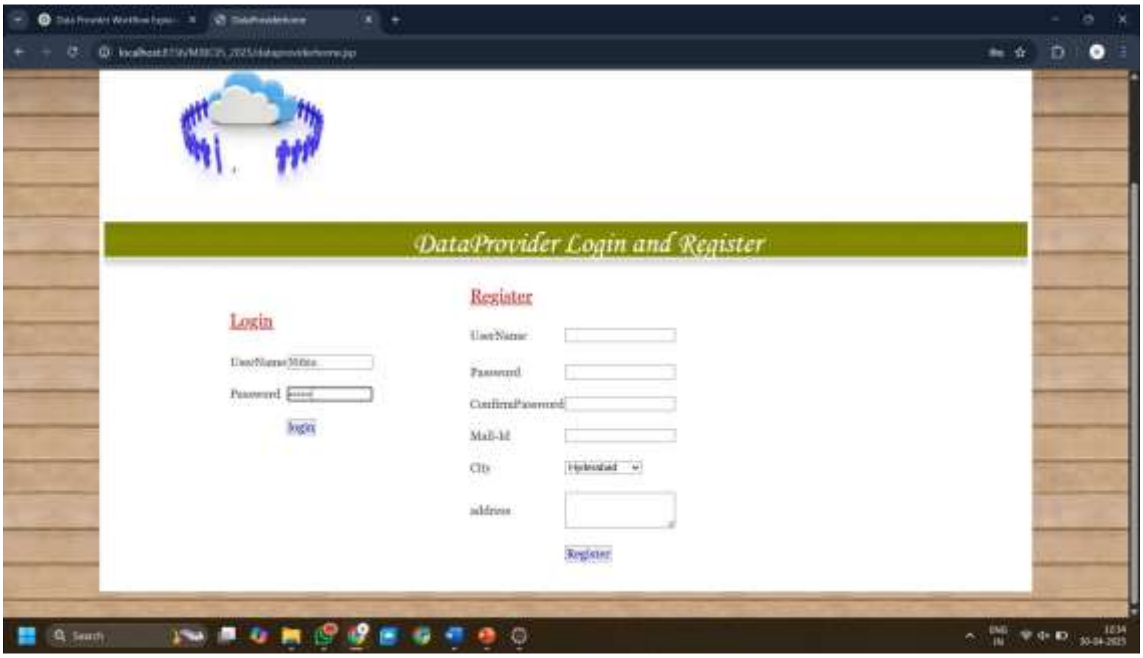
10. RESULTS:



Securing Cloud Data with Blockchain Based Approach

Figure-2: Home Page

The image displays a dashboard interface for Securing Cloud Data with Blockchain Based Approach designed to safeguard cloud-stored information using blockchain technology. The interface includes a clean header with navigation links for different user roles—Home Page, DataProvider, DataUtilizer, Authenticator, and Contact Us—enabling role-based access. The page is visually enhanced with a space-themed background, adding a futuristic and secure feel to the application. The presence of localhost in the URL indicates it's currently running on a local server for development or testing purposes.



DataProvider Login and Register

Login

UserName Mithin

Password

Register

UserName

Password

ConfirmPassword

Mail-Id

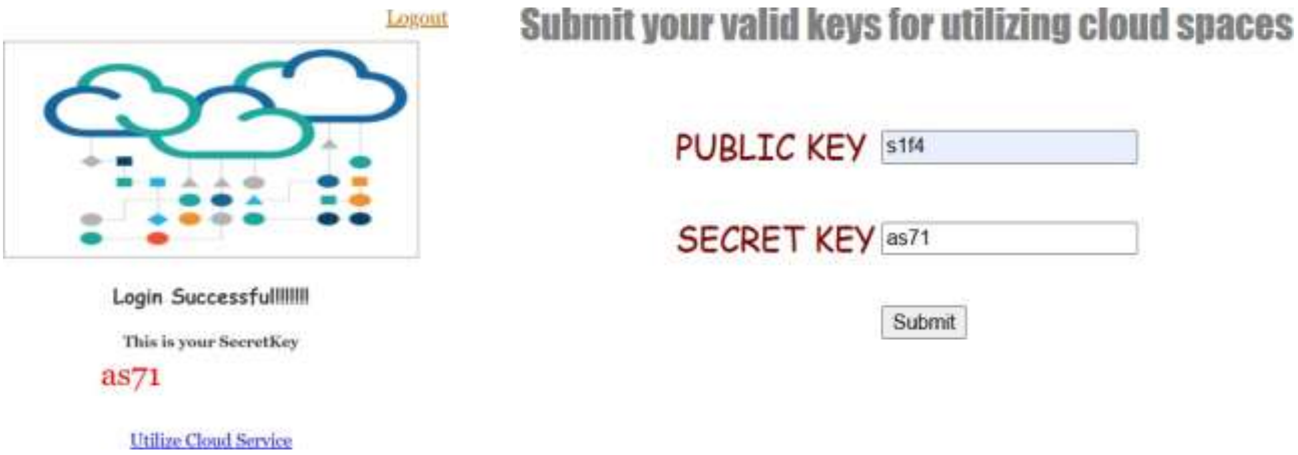
City Hyderabad

address

Figure-3: Data Provider register and login:

The image shows the **Data Provider Login and Register** page, which allows users to either log in with existing credentials or register a new account. The page is divided into two sections: **Login** on the left, where users enter their username and password, and **Register** on the right, where new users provide details like username, password, email, city (with a dropdown), and address.

A green header labelled *"Data Provider Login and Register"* separates the sections clearly. The interface is simple and user-friendly. A similar Login and Register page is also available for **Data Utilizer**, maintaining consistency across both modules.



Login Successfull!!!!!!

This is your SecretKey

as71

Submit your valid keys for utilizing cloud spaces

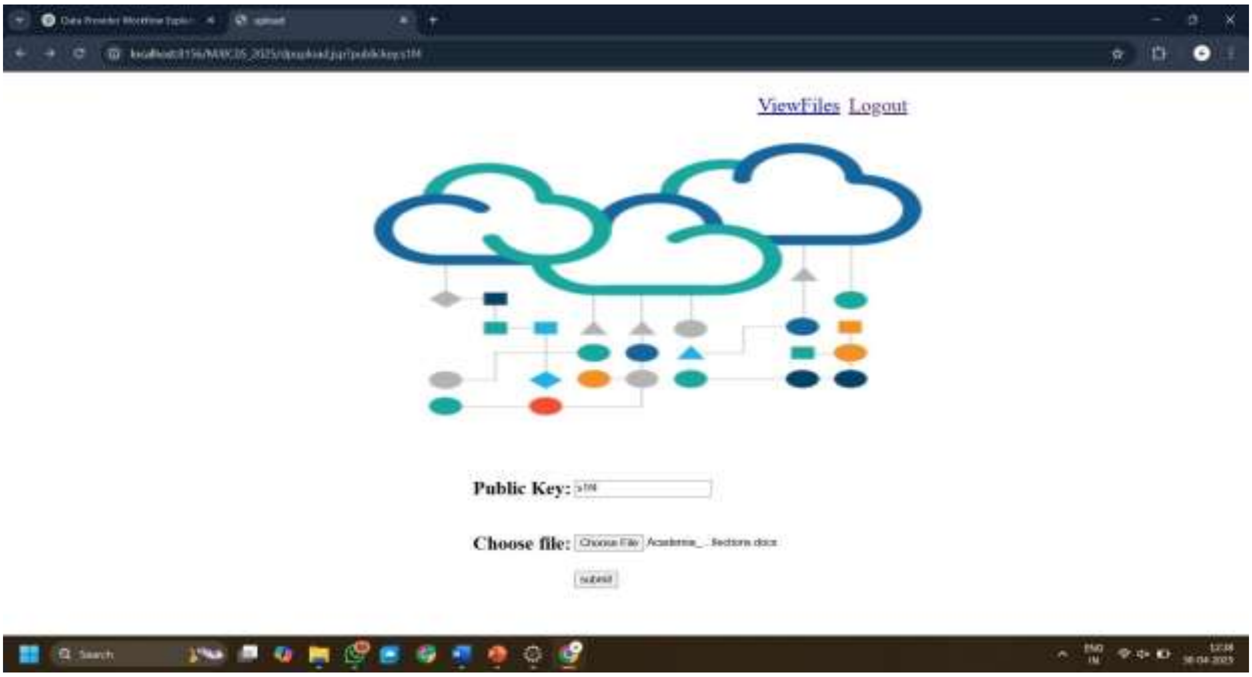
PUBLIC KEY: s1f4

SECRET KEY: as71

Figure-4: Secret Key Generation

The first image confirms a **successful login** after valid keys are submitted. It displays a message saying *"Login Successful"*, shows the **Secret Key**, and provides a link labeled **"Utilize Cloud Service"** for the next step. A **Logout** option is available at the top for ending the session. These keys are used to securely authorize access to cloud resources.

The second image shows a **key submission form** where users are prompted to enter their **Public Key** and **Secret Key** to access cloud services. The keys are entered into clearly labeled input fields, and a **Submit** button is provided below to proceed with the authentication.



localhost:8156/MAIC05_2025/dpupload.jsp?publickey=s1f4

Public Key: s1f4

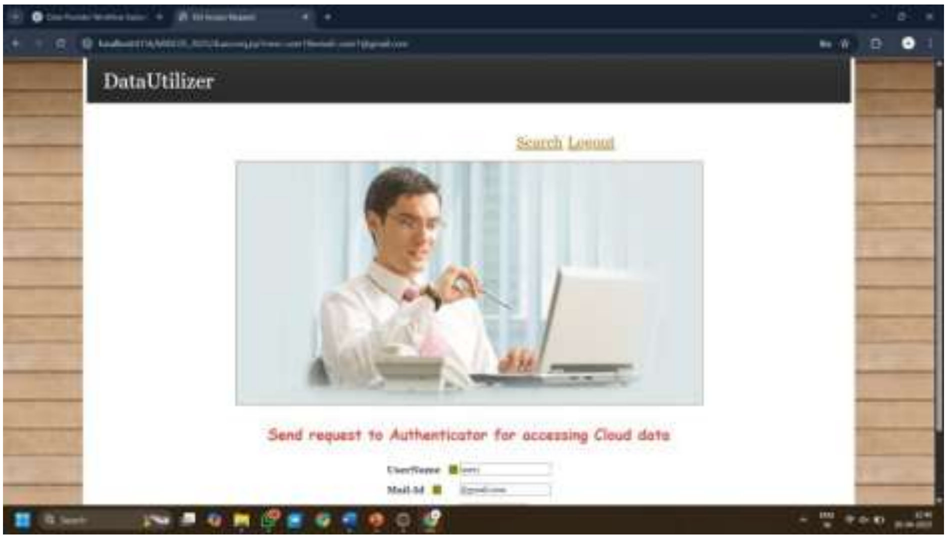
Choose file: Academia_...Sections.docx

Figure-5: Uploading Files

The image shows a file upload interface for the Data Provider module, where users can upload files to the cloud using their Public Key as identification.

Below that, there is a Choose file button allowing users to select a file from their system - in this case, a .docx file has been selected. A Submit button is provided to upload the chosen file.

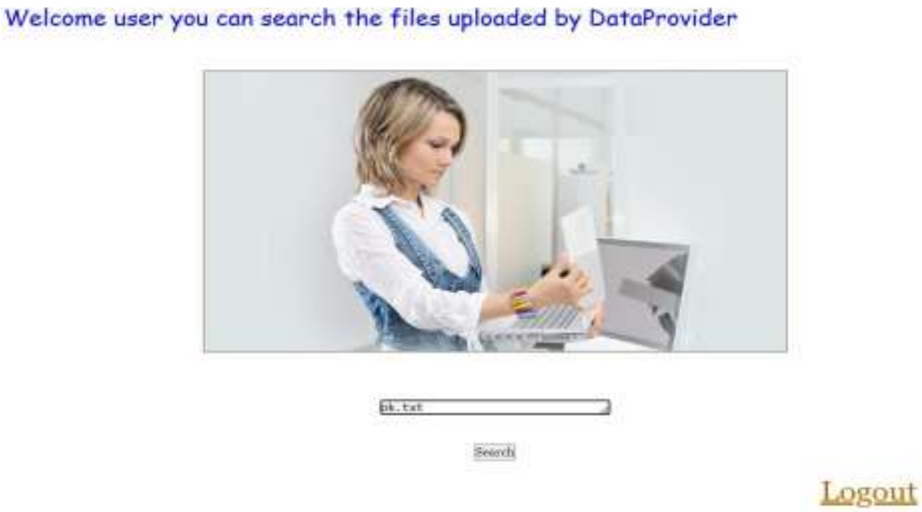
Additionally, the top-right corner of the page contains links to ViewFiles (for viewing uploaded files) and Logout, helping users navigate or end their session. This interface ensures that only authenticated users with a valid key can upload content to the cloud.



Send request to Authenticator for accessing Cloud data

UserName:
Mail-Id:

Figure-6: Data Utilizer



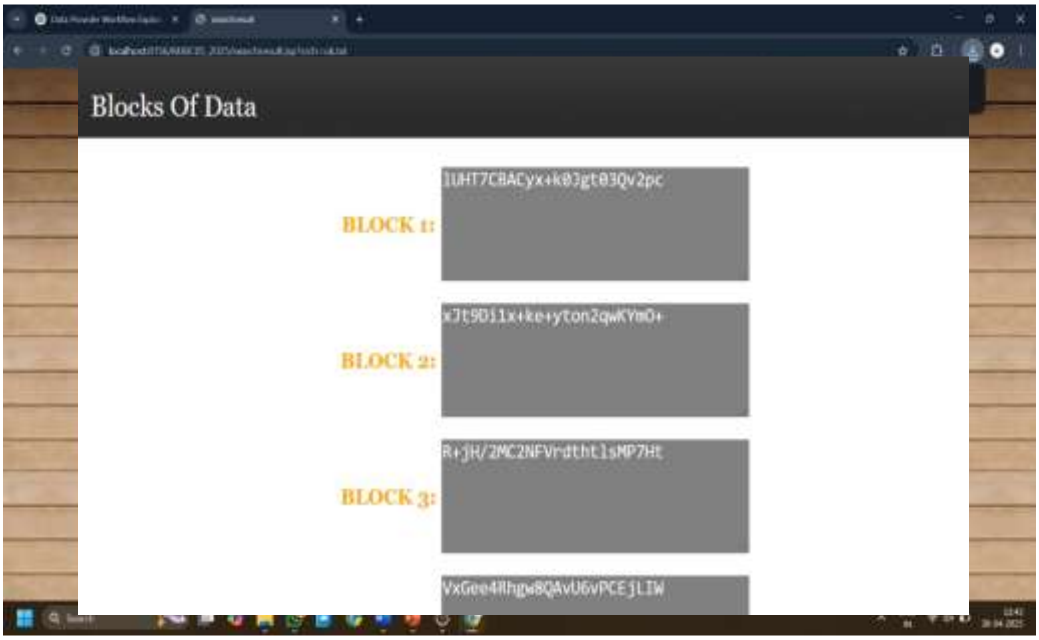
Welcome user you can search the files uploaded by DataProvider

bk.txt

Figure-7: Logout

The first image shows the **Data Utilizer access request page**, where a user can send a request to the authenticator to access cloud data. It includes fields for entering the **Username** and **Mail-Id**, along with a button to initiate the request.

The second image displays the **file search page** for Data Utilizers. After receiving access, users can **search for files uploaded by Data Providers** by entering the file name in the input box and clicking the **Search** button. A Logout link is also available.



Blocks Of Data

BLOCK 1: lUHT7CBACyx+k0JgtB3Qv2pc

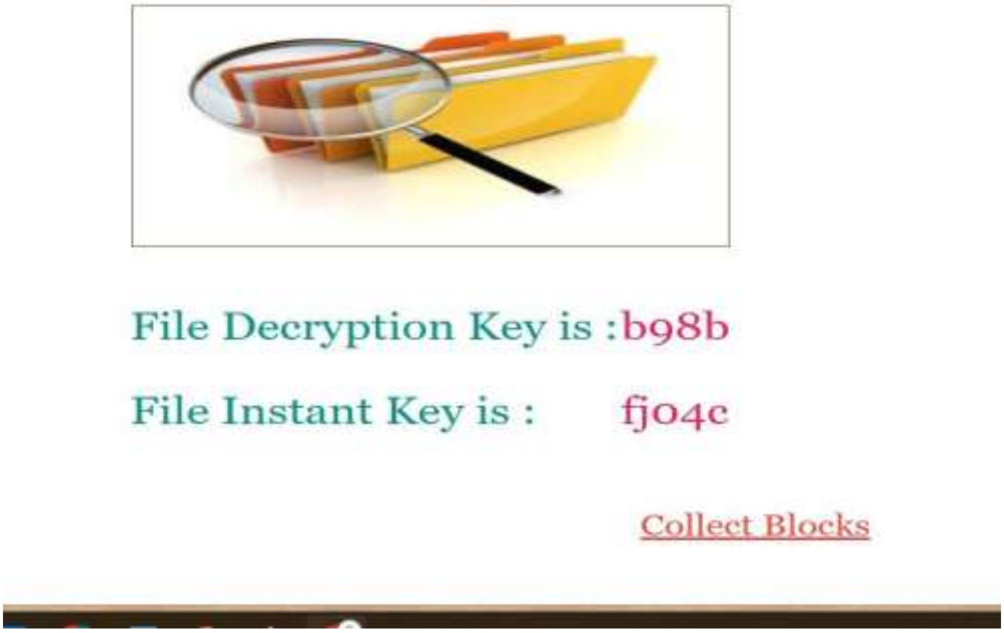
BLOCK 2: xJt9D11x+ke+yton2qwKYmO+

BLOCK 3: R+jH/2MC2NFVrdthtlsMP7Ht

VxGee4RhgwBQAvU6vPCEjLIW

Figure-8: Downloading Encrypted File

This image shows the search result page for the Data Utilizer. After searching for a file, the matching file is listed with its name and the user can download the encrypted file. The user also has options to Decrypt the file or Logout.



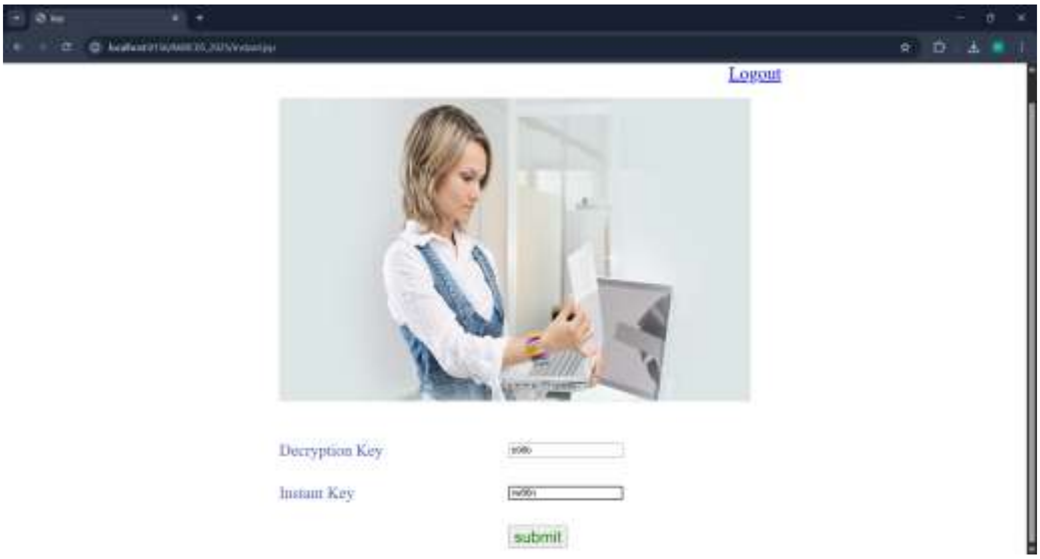
File Decryption Key is :b98b

File Instant Key is : fjo4c

Figure-9: Decrypting File

When the user tries to decrypt the file they get a Decryption Key and a Instant Key then they can collect the blocks the encrypted data file and decrypt them using the keys provided.

Figure-10: Block of Data



Decryption Key [illegible]

Instant Key [illegible]

Figure-11: Actual File retrieval

After successfully collecting the blocks click on next and you will be directed to this page shown in the image where you are required to provide the keys and download the actual file uploaded by the provider.

11. CONCLUSION

This paper proposes a cloud-assisted attribute-based searchable encryption scheme on the blockchain. The system in this paper uses attribute-based encryption technology to enable data owners to perform fine- grained search authorization for data users. Use searchable encryption technology to complete the search of keywords on the blockchain and realize the secure access of data users to encrypted data. During the process, no vital information about keywords and data files will be leaked to the cloud server. We give detailed correctness proofs, performance analyses and security proofs. Numerical experiment results show that the proposed scheme has high efficiency.

12. FUTURE ENHANCEMENTS

In future work, we consider combining proxy re-encryption technology to apply it in electronic medical record data sharing to realize data sharing with third-party data users.

REFERENCES

1. F. Nzanywayingoma and Y. Yang, "Efficient resource management techniques in cloud computing environment: A review and discussion", Int. J. Comput. Appl., vol. 41, no. 3, pp. 165-182, May 2019.
2. M. Li, S. Yu, N. Cao and W. Lou, "Authorized private keyword search over encrypted data in cloud computing", Proc. 31st Int. Conf. Distrib. Comput. Syst., pp. 383-392, Jun. 2011.
3. C. Bösch, P. Hartel, W. Jonker and A. Peter, "A survey of provably secure searchable encryption", ACM Comput. Surv., vol. 47, no. 2, pp. 1-51, Jan. 2015.
4. J. Sun, D. Chen, N. Zhang, G. Xu, M. Tang, X. Nie, et al., "A privacy-aware and traceable fine-grained data delivery system in cloud-assisted healthcare IIoT", IEEE Internet Things J., vol. 8, no. 12, pp. 10034- 10046, Jun. 2021.
5. J. Gao, H. Yu, X. Zhu and X. Li, "Blockchain-based digital rights management scheme via multi authority ciphertext-policy attribute-based encryption and proxy re-encryption", IEEE Syst. J., vol. 15, no. 4, pp. 5233-5244, Dec. 2021.
6. Y. Hei, J. Liu, H. Feng, D. Li, Y. Liu and Q. Wu, "Making MA-ABE fully accountable: A blockchain- based approach for secure digital right management", Comput. Netw., vol. 191, May 2021.
7. H. Yin, J. Zhang, Y. Xiong, L. Ou, F. Li, S. Liao, et al., "CP-ABSE: A ciphertext-policy attribute-based searchable encryption scheme", IEEE Access, vol. 7, pp. 5682-5694, 2019.

8. Q. Chai and G. Gong, "Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers", Proc. IEEE Int. Conf. Commun. (ICC), pp. 917-922, Jun. 2012.
9. C. Li, M. Dong, J. Li, G. Xu, X.-B. Chen, W. Liu, et al., "Efficient medical big data management with keyword-searchable encryption in health chain", IEEE Syst. J., vol. 16, no. 4, pp. 5521-5532, Dec. 2022.
10. Z. Zhang, J. Zhang, Y. Yuan and Z. Li, "An expressive fully policy-hidden ciphertext policy attribute- based encryption scheme with credible verification based on blockchain", IEEE Internet Things J., vol. 9, no. 11, pp. 8681-8692, Jun. 2022.
11. Y. He, H. Wang, Y. Li, K. Huang, V. C. M. Leung, F. R. Yu, et al., "An efficient ciphertext-policy attribute-based encryption scheme supporting collaborative decryption with blockchain", IEEE Internet Things J., vol. 9, no. 4, pp. 2722-2733, Feb. 2022.
12. K. Routray, K. Sethi, B. Mishra, P. Bera and D. Jena, "CP-ABE with hidden access policy and outsourced decryption for cloud-based EHR applications" in Information and Communication Technology for Intelligent Systems, Singapore: Springer, vol. 2, 2021.
13. S. Mashhadi, "Secure publicly verifiable and proactive secret sharing schemes with general access structure", Inf. Sci., vol. 378, pp. 99-108, Feb. 2017.
14. P.-C. Chen, T.-H. Kuo and J.-L. Wu, "A study of the applicability of ideal lattice-based fully homomorphic encryption scheme to Ethereum blockchain", IEEE Syst. J., vol. 15, no. 2, pp. 1528-1539, Jun. 2021.
15. B. B. Gupta, K.-C. Li, V. C. M. Leung, K. E. Psannis and S. Yamaguchi, "Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system", IEEE/CAA J. Autom. Sinica, vol. 8, no. 12, pp. 1877-1890, Dec. 2021.
16. M. Chen, "Discussion on implementation and application of RSA algorithm in smart card operating system", Proc. Int. Conf. High Perform. Comput. Commun. (HPCCE), pp. 1-6, Feb. 2022.
17. S. Yaji, K. Bangera and B. Neelima, "Privacy preserving in blockchain based on partial homomorphic encryption system for ai applications", Proc. IEEE 25th Int. Conf. High Perform. Comput. Workshops (HiPCW), pp. 81-85, Dec. 2018.
18. P. P. Nayudu and K. R. Sekhar, "Accountable specific attribute-based encryption scheme for cloud access control", Int. J. Syst. Assurance Eng. Manage., vol. 2022, pp. 1-10, Jul. 2022.
19. Y. Yang, M. Hu, Y. Cheng, X. Liu and W. Ma, "Keyword searchable encryption scheme based on blockchain in cloud environment", Proc. 3rd Int. Conf. Smart BlockChain (SmartBlock), pp. 1-4, Oct. 2020.
20. Y. Zhang, C. Xu, J. Ni, H. Li and X. S. Shen, "Blockchain-assisted public-key encryption with keyword search against keyword guessing attacks for cloud storage", IEEE Trans. Cloud Comput., vol. 9, no. 4, pp. 1335-1348, Oct. 2021.
21. S. Liu, J. Yu, Y. Xiao, Z. Wan, S. Wang and B. Yan, "BC-SABE: Blockchain-aided searchable attribute- based encryption for cloud-IoT", IEEE Internet Things J., vol. 7, no. 9, pp. 7851-7867, Sep. 2020.
22. S. Tahir and M. Rajarajan, "Privacy-preserving searchable encryption framework for permissioned blockchain networks", Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData), pp. 1628-1633, Jul. 2018.
23. S. Jiang, J. Cao, J. A. McCann, Y. Yang, Y. Liu, X. Wang, et al., "Privacy-preserving and efficient multi-keyword search over encrypted data on blockchain", Proc. IEEE Int. Conf. Blockchain (Blockchain),pp. 405-410, Jul. 2019.
24. X. Yan, X. Yuan, Q. Ye and Y. Tang, "Blockchain-based searchable encryption scheme with fair payment", IEEE Access, vol. 8, pp. 109687-109706, 2020.
25. B. Chen, D. He, N. Kumar, H. Wang and K. R. Choo, "A blockchain-based proxy re-encryption with equality test for vehicular communication systems", IEEE Trans. Netw. Sci. Eng., vol. 8, no. 3, pp. 2048- 2059, Jul. 2021.
26. J. Han, Z. Li, J. Liu, H. Wang, M. Xian, Y. Zhang, et al., "Attribute-based access control meets blockchain-enabled searchable encryption: A flexible and privacy-preserving framework for multi-user search", Electronics, vol. 11, no. 16, pp. 2536, Aug. 2022.
27. S. Wang, X. Wang and Y. Zhang, "A secure cloud storage framework with access control based on blockchain", IEEE Access, vol. 7, pp. 112713-112725, 2019.
28. R. Awadallah, A. Samsudin, J. S. Teh and M. Almazrooie, "An integrated architecture for maintaining security in cloud computing based on blockchain", IEEE Access, vol. 9, pp. 69513-69526, 2021.

29. M. Whaiduzzaman, J. N. Mahi, A. Barros, I. Khalil, C. Fidge and R. Buyya, "BFIM: Performance measurement of a blockchain based hierarchical tree layered fog-IoT microservice architecture", IEEE Access, vol. 9, pp. 106655-106674, 2021.

30. Y. Sun, X. Li, F. Lv and B. Hu, "Research on logistics information blockchain data query algorithm based on searchable encryption", IEEE Access, vol. 9, pp. 20968-20976, 2021.

31. R. Guo, H. Shi, D. Zheng, C. Jing, C. Zhuang and Z. Wang, "Flexible and efficient blockchain-based ABE scheme with multi-authority for medical on demand in telemedicine system", IEEE Access, vol. 7,pp. 88012-88025, 2019.

32. S. Liu, J. Yu, L. Chen and B. Chai, "Blockchain-assisted comprehensive key management in CP-ABE for cloud-stored data", IEEE Trans. Netw. Service Manage., no. 2, pp. 1745-1758, Jun. 2023.