IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 5, June 2025

Impact Factor: 7.67

Content-Aware Secure Search Using Attribute Based Encryption IoT Cloud Platforms

Mr. K. Vigneshwar[1] , Ms. G. Sanjana[2] , Ms. B. Vasavi[3], Mr. B. Bhagyavan[4]

Assistant Professor, Department of CSE[1]

Students, Department of CSE[2,3,4]

Guru Nanak Institute of Technology, Hyderabad, Telangana

Abstract: *The integration of cloud computing with Internet of Things (IoT) devices offers vast opportunities for scalable data storage and real-time services. However, it also introduces critical security and privacy challenges, particularly in ensuring fine-grained access control and secure data retrieval. This paper proposes a context-aware secure search framework using Attribute-Based Encryption (ABE) tailored for IoT-cloud platforms. The system enables encrypted data to be searched efficiently without revealing sensitive content or search patterns, leveraging context-aware policies to enhance access control flexibility. Additionally, the scheme supports forward security, ensuring past data remains protected even if current keys are compromised. Experimental analysis demonstrates the framework's effectiveness in maintaining data confidentiality, reducing computational overhead, and ensuring practical usability in resource-constrained IoT environments.*

Keywords: Internet of Things

I. INTRODUCTION

The rapid advancement of Internet of Things (IoT) technology has led to its integration into many aspects of daily life, including smart homes, healthcare, transportation, and industry. As IoT devices become more prevalent, they generate vast amounts of data. Analyzing and predicting patterns within this data can significantly improve healthcare, disaster forecasting, service quality, and resource management. However, IoT devices have limited processing and storage capabilities, making it difficult for them to manage such large datasets. To address this, cloud-assisted IoT has emerged, leveraging the cloud's robust storage and computing power at a relatively low cost.To ensure the security of data stored in semi-trusted cloud environments, an encryption-before-outsourcing approach is often used. While this protects data confidentiality, it complicates the ability to search through encrypted data. Searchable Encryption (SE) addresses this issue by enabling keyword searches over encrypted content. Moreover, managing access to large volumes of encrypted data in the cloud poses additional challenges. Ciphertext-Policy Attribute-Based Searchable Encryption (CP-ABSE) addresses this by combining one-to-many encryption, fine-grained access control, and keyword search functionality, allowing data owners to manage and retrieve data securely and efficiently.In this framework, data collected by IoT devices is encrypted and tagged with searchable indexes before being uploaded to the cloud. When the data owner wants to retrieve specific information, they send a trapdoor (a special search token) to the cloud. The cloud server then returns matching results only if the search attributes align with the ciphertext's access policy and keywords.However, CP-ABSE still faces security concerns, especially regarding the secure deletion of sensitive data that is no longer needed. Relying on the cloud to delete data is risky, as cloud providers may retain copies for profit. Achieving secure and independent data deletion remains a complex task. A promising approach involves regularly updating trapdoors to revoke the ability to search specific ciphertexts, thereby making the deleted data inaccessible without needing cloud cooperation.Although data deletion has been explored in other cryptographic schemes, it has not been fully addressed within CP-ABSE. Prior work includes Green and Miers' Puncturable Encryption (PE), where secret keys can be "punctured" to lose decryption ability for data associated with certain labels. Other efforts include Phuong et al.'s Puncturable Attribute-Based Encryption (Pun-ABE) and the Pun-SSE scheme that combines Searchable Symmetric Encryption with PE to enable secure deletion.To bridge the gap in CP-ABSE, we propose a novel scheme called

DOI: 10.48175/IJARSCT-27701

Puncturable Ciphertext-Policy Attribute-Based Searchable Encryption (Pun-CP-ABSE). This mechanism integrates PE into CP-ABE and adds searchable functionality. In our approach, the data owner generates two types of trapdoors: a general trapdoor for searching and a puncturable trapdoor for secure data deletion. The general trapdoor allows access-controlled searches, while the puncturable trapdoor, derived from a PE secret key, supports fine-grained deletion using a puncture algorithm. Once punctured with specific tags, the trapdoor loses the ability to retrieve matching ciphertexts, effectively ensuring that deleted data becomes inaccessible.

The key contributions of Pun-CP-ABSE are:

1. We introduce a Pun-CP-ABSE scheme that supports precise, permanent, fine-grained, and self-managed data deletion within a searchable CP-ABE framework, without relying on trusted third parties and while ensuring forward security.
2. The scheme maintains fine-grained access control and searchable encryption, enabling data owners to retrieve relevant encrypted data only if their attributes satisfy the access structure.
3. We demonstrate the scheme's security under Chosen-Plaintext and Chosen-Keyword Attacks (CPA and CKA), and validate its practicality and efficiency through simulation experiments.

II. LITERATURE SURVEY

Title: Multiauthority CP-ABE-based access control model for iot-enabled healthcare infrastructure

Author: S. Das and S. Namasudra

Year: 2024

Description: With the rapid expansion of Internet of Things (IoT) technologies, ensuring strong data security has become more important than ever. Since IoT devices constantly transmit data over the Internet, protecting that data is absolutely critical.One promising approach to securing IoT data is fine-grained access control, which can be achieved using ciphertext-policy attribute-based encryption (CP-ABE). However, many existing CP-ABE schemes rely on bilinear pairing operations, which are computationally intensive and not ideal for resource-constrained IoT devices. To address this, we propose a CP-ABE scheme based on elliptic curve cryptography (ECC), which offers faster computation and is better suited for lightweight environments. Our proposed scheme also introduces multiple attribute authorities to manage attributes and key generation. This distributes the workload and avoids the bottleneck of relying on a single authority, as seen in traditional CP-ABE systems. Furthermore, to reduce the computational burden on end-users, we outsource part of the decryption process to a user-assisting entity.To validate the approach, we conduct both formal security analysis and performance comparisons. The results show that our scheme outperforms several well-known methods in terms of both security and efficiency.

Title: Extracting spatial information of IoT device events for smart home safety monitoring,

Author: Y. Wan, X. Lin, K. Xu, F. Wang, and G. Xue,

Year: 2023

Description: Smart home IoT devices are now common in households, powering a wide range of applications—from intelligent home automation to connected healthcare and security surveillance. These devices generate a wealth of network traffic data, which has been instrumental in advancing research on smart home network behavior.However, because most smart home devices rely on cloud-based communication, and traffic data at the cloud end is often inaccessible, there's been limited progress in understanding *where* a device event actually occurs. In other words, it's still a challenge to determine whether an event was triggered locally within the home or remotely via the cloud.In this paper, we explore the difficulties of extracting spatial information from IoT device events by analyzing how smart home devices typically communicate. We introduce **IoTDuet**, a system designed to distinguish between locally and remotely triggered device events. IoTDuet takes advantage of a key insight: controlling devices like smartphones and tablets tend to use stable domain names when they send commands to the cloud from the home network. Finally, we demonstrate how identifying the location of device triggers can play a vital role in smart home safety monitoring and related applications.

DOI: 10.48175/IJARSCT-27701

Title: Verifiable outsourced attribute-based encryption scheme for cloud-assisted mobile e-health system
Author: Y. Miao, F. Li, X. Li, J. Ning, H. Li, K. R. Choo, and R. H. Deng,
Year: 2023
Description: Cloud-assisted mobile electronic health (e-health) systems make it easier for patients and healthcare providers to share health data—but they also raise serious concerns about data security and privacy. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is a promising solution for enforcing fine-grained access control over encrypted health data. However, traditional CP-ABE schemes can be too heavy for mobile devices like smartphones and sensors, leading to high encryption and decryption overhead.There's also the risk of untrusted cloud servers acting maliciously—whether by leaking sensitive data, cutting corners to save on computation and storage, or mishandling encryption tasks. To address these challenges, this paper introduces an **Outsourced CP-ABE (OABE) scheme with verifiable encryption.** By splitting secret keys across an attribute set and using short digital signatures, the scheme lightens the load on mobile users while ensuring that cloud servers execute encryption correctly. Building on this, we present an enhanced version called **OABE+**, which adds **verifiable decryption** through a tag-based verification mechanism. This ensures that even the ciphertext transformation carried out by the cloud can be trusted. Our formal security analysis confirms that both schemes are resistant to unauthorized access and malicious behavior. Additionally, experiments using real-world datasets show that our proposed solutions are not only secure but also practical and efficient for real-world use.

III. METHODOLOGY

EXISTING SYSTEM

We prove that the Pun-CP-ABSE scheme is secure under the Chosen-Plaintext Attack (CPA) and Chosen Keyword Attack (CKA). Furthermore, we present the efficiency and practicability of the Pun-CP-ABSE scheme by implementing simulations.In our scheme, the data owner generates two kinds of trapdoors named general trapdoor and puncturable trapdoor, respectively, for searching and securely deleting the outsourced data.They efficiently achieve user-level revocation and give proof of resisting CKA and Keyword Guessing Attack.

EXISTING SYSTEM DISADVANTAGES

- This has a larger key space and more complex structures.
- By dividing the encryption process and searching for matches in intermediate results.

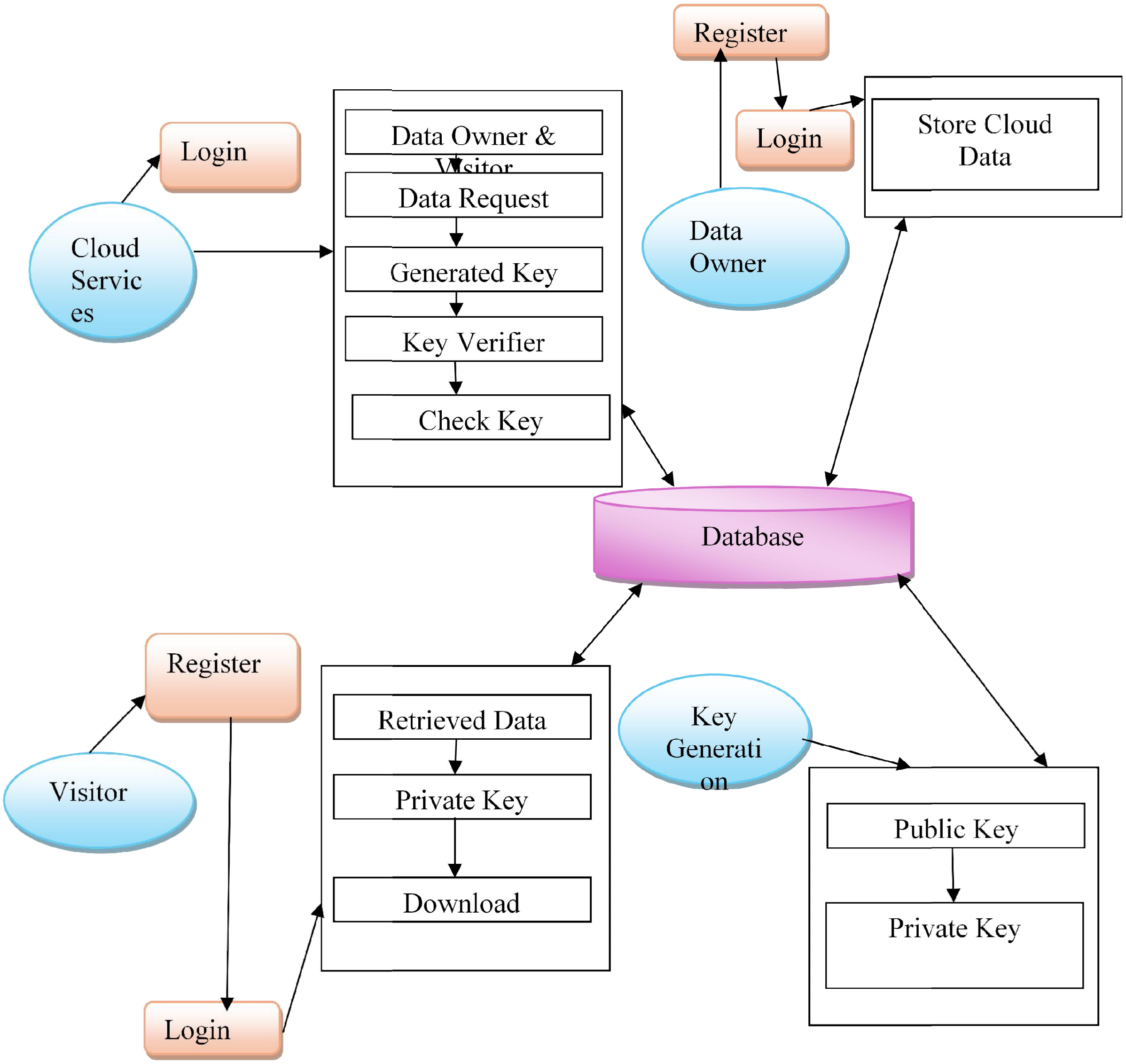
PROPOSED SYSTEM

We propose a Puncturable CP-ABSE (Pun CP-ABSE) scheme that achieveselfcontrolled data deletion with a fine-grained access structure under the searchable mechanism. The data owner punctures the trapdoor to accomplish the data deletion. Then, the deletion process does not need to communicate with a trusted third party and can guarantee forward security. After the punctuation, the cloud server can no longer search for the corresponding cipher text We prove that the Pun-CP-ABSE scheme is secure under the Chosen-Plaintext Attack (CPA) and Chosen Keyword Attack (CKA). Furthermore, we present the efficiency and practicability of the Pun-CP-ABSE scheme by implementing simulations.

PROPOSED SYSTEM ADVANTAGES

- The data looks for matches between the intermediate cipher text.
- The output hash value is always the same for a given input.
- The system allows secure and fine-grained data deletion.
- It ensures forward security for deleted data.

IV. SYSTEM ARCHITECTURE



MODULES:

1.User Interface Design

In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.

2. Cloud Services

Cloud services has an id and password. Cloud services has a details of a data owner and visitor details. The cloud services have a data request to share a data. The cloud services has a key generate a key. The cloud services has a key

DOI: 10.48175/IJARSCT-27701

verifier to share a data. The cloud services has a check a key to download whether the cloud services key are match the decrypt a visitor.

3. Data Owner

The data owner has a register with a detail. The data owner has a login with a user id and password. The data owner has a store a cloud data to share in a database.

4. Visitor

The Visitor module has a register with all details. The visitor has a login with a user id and password. The visitor has a retrieved a data to get from a data owner. The visitor have a private key to generated a data. The private key has a verify a cloud services if the private key has match the data will be decrypt a data.

Key Generation Center

The **Key Generation Center (KGC)** plays a crucial role in the system, acting as a trusted authority responsible for generating and managing cryptographic keys. It consists of five functional modules and maintains both a public key and a private key, which are used to securely share data within a database environment.

V. IMPLEMENTATION

Attribute-based encryption Algorithm

This project uses the **Attribute-Based Encryption (ABE)** scheme, a powerful public-key encryption method that enables **fine-grained access control** over encrypted data. Unlike traditional encryption, which grants access based on specific user identities, ABE grants access based on a user's attributes (such as role, department, or clearance level).There are two main types of ABE, classified according to where the access structure is embedded:

- **Key-Policy ABE (KP-ABE):** The access policy is embedded in the user’s private key.
- **Ciphertext-Policy ABE (CP-ABE):** The access policy is defined in the ciphertext, allowing data owners to control who can access their data.

The fine-grained nature of ABE makes it especially well-suited for use in **cloud environments,** where scalable and flexible access control is essential. Because of its potential, ABE has attracted significant research interest, leading to the development of several variants and enhancements for different application needs.

Components of the ABE Algorithm

Key Generation:

The **Attribute Authority (AA)** generates a master public key and a master private key. These keys are used to issue attribute-based certificates to users and to encrypt data according to defined policies.

Encryption:

The **data owner** encrypts the data using the master public key and a chosen set of attributes that define the **access policy**. Only users whose attributes match this policy can decrypt and access the data.

CP-ABSE Algorithm (Ciphertext-Policy Attribute-Based Searchable Encryption)

CP-ABSE (Ciphertext-Policy Attribute-Based Searchable Encryption) is an advanced cryptographic scheme that combines the principles of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and Searchable Encryption (SE). It allows users to securely search encrypted data stored in the cloud, where access and search capabilities are controlled by a defined access policy based on user attributes.

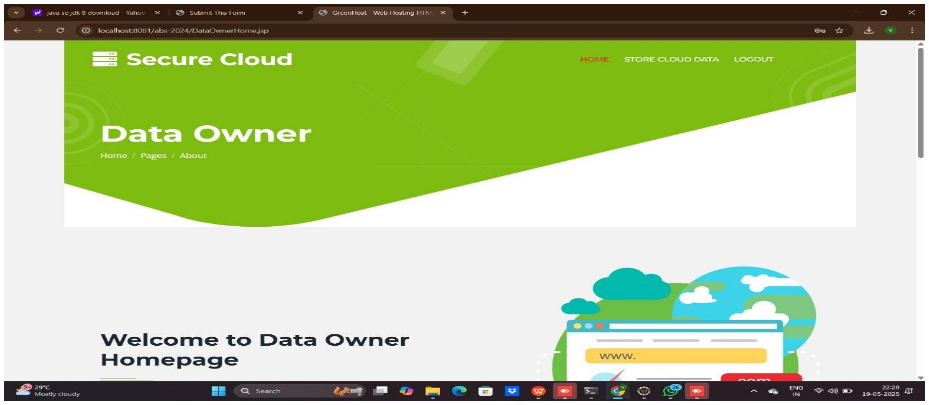
Key Features:

- **Attribute-Based Access Control:** Data is encrypted under an access policy. Only users whose attributes satisfy the policy can decrypt or search the data.

- **Searchable Encryption:** Enables keyword-based search over encrypted data. The cloud server can perform search operations without learning the content or keywords.
- **Ciphertext-Policy Approach:** Access policy is embedded in the ciphertext (data owner defines the policy).

VI. EXPERIMENTAL RESULTS

Data Owner

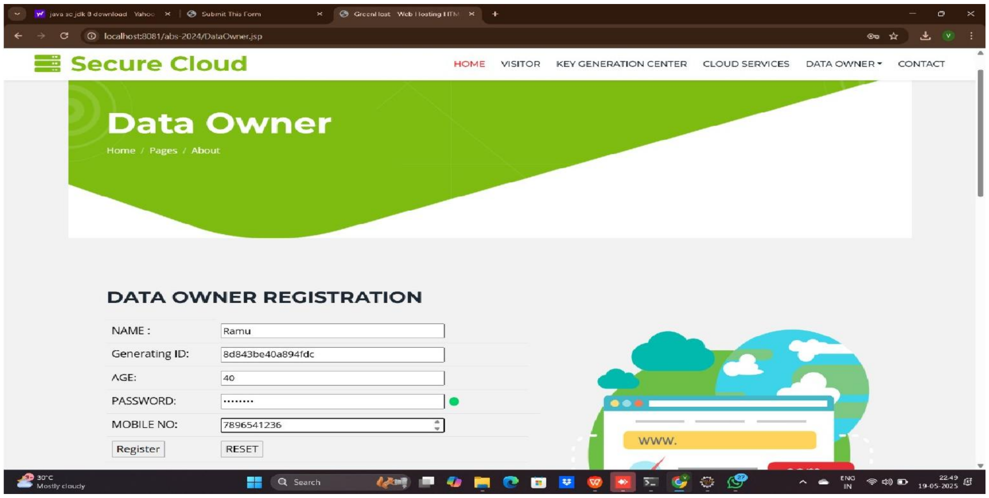


Welcome to Data Owner Homepage

EXPLANATION:

The displayed figure represents the Data Owner Homepage of a secure cloud storage system. It is part of the first step in the workflow where the data owner, after successful registration and login, accesses their dedicated dashboard.
page.

Data owner Registration



DATA OWNER REGISTRATION

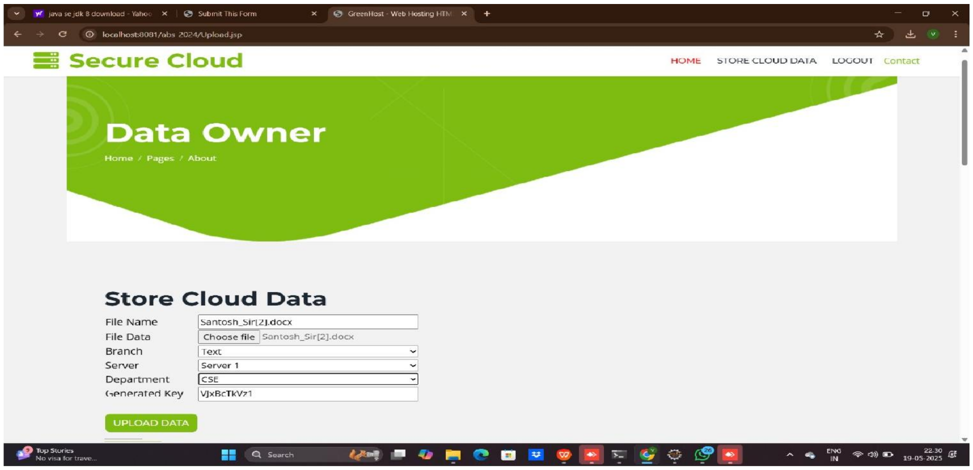
NAME :	Ramu
Generating ID:	8d843be40a894fdc
AGE:	40
PASSWORD:	••••••••
MOBILE NO:	7896541236
Register	RESET

EXPLANATION:

The second figure illustrates the Data Owner Registration page in the Secure Cloud application, which is a crucial part of STEP 1: DATA OWNER REGISTER This interface allows a new data owner to create an account by filling in essential personal and security information.

DOI: 10.48175/IJARSCT-27701

Cloud data Storage



Store Cloud Data

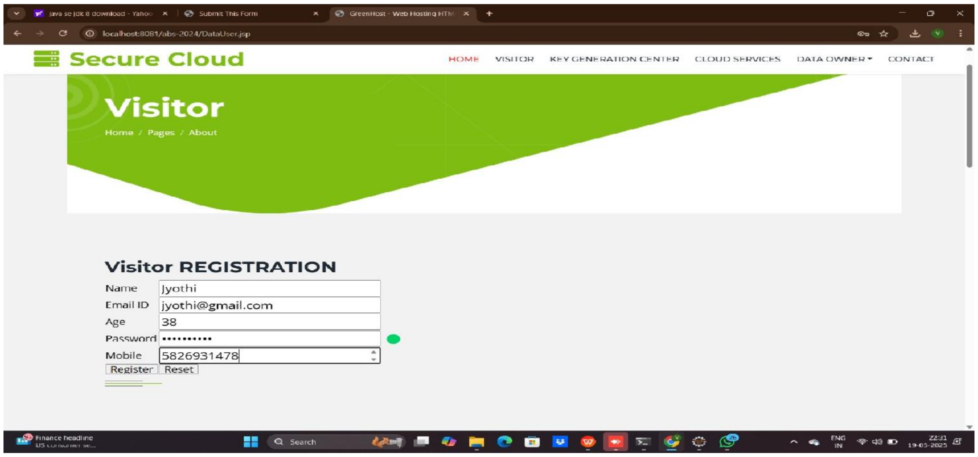
File Name	Santosh_Sir[2].docx
File Data	Choose file Santosh_Sir[2].docx
Branch	Text
Server	Server 1
Department	CSE
Generated Key	VJxBcTkVz1

UPLOAD DATA

EXPLANATION:

The image displays a web interface titled "Secure Cloud" with "Data Owner" as the main section. The current page is "Store Cloud Data," and it presents a form for uploading files.

Visitor Registration



Visitor REGISTRATION

Name	Jyothi
Email ID	jyothi@gmail.com
Age	38
Password	••••••••••
Mobile	5826931478

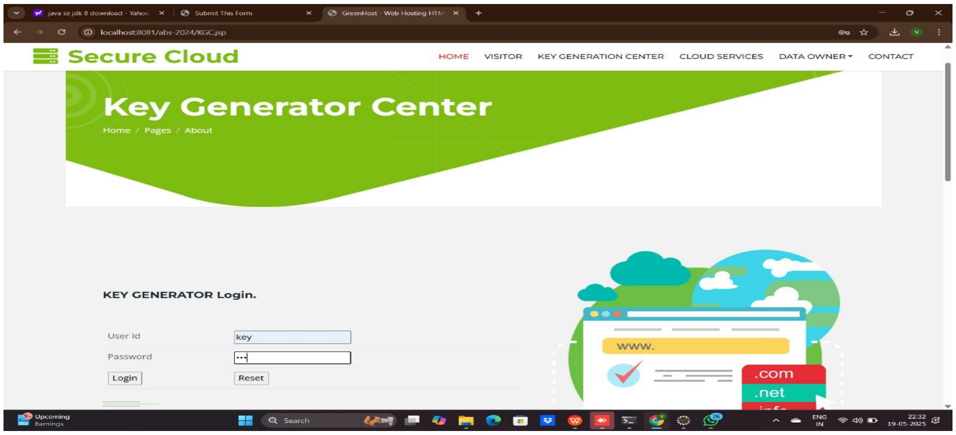
Register Reset

EXPLANATION:

This represents registration page for "Visitors" within a "Secure Cloud" application. Users are required to provide their name, email, age, password, and mobile number to register. The application appears to be running in a local development environment.

DOI: 10.48175/IJARSCT-27701

Key Generation Center



Key Generator Center

KEY GENERATOR Login.

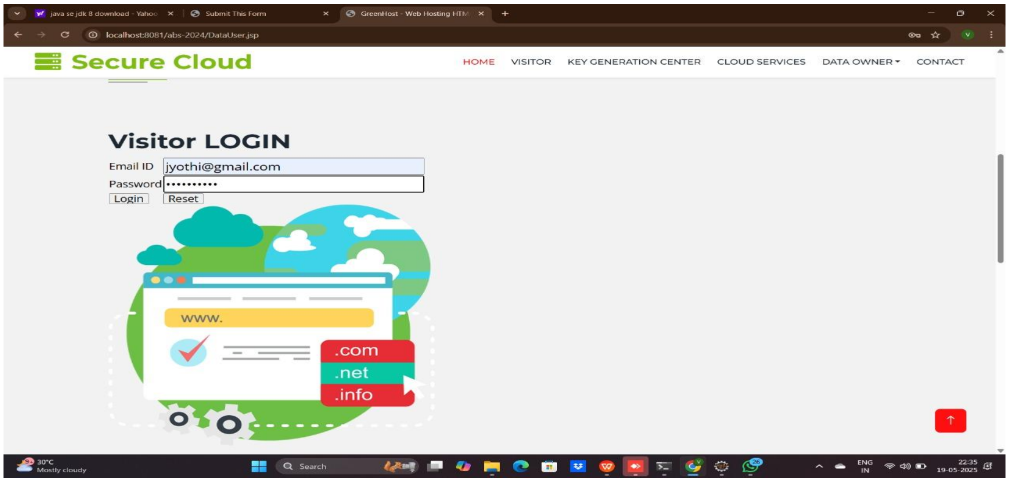
User Id: key
Password: •••

Login Reset

EXPLANATION:

In essence, it illustrate the user interfaces for key stages of the "Secure Cloud" system, including data upload by owners, visitor registration, and access to a key generation facility, all of which are part of a multi-step process outlined in the accompanying documentation. The user id and password is for login the key generator is key by default.

Visitor Login



Visitor LOGIN

Email ID: jyothi@gmail.com
Password: ••••••••••

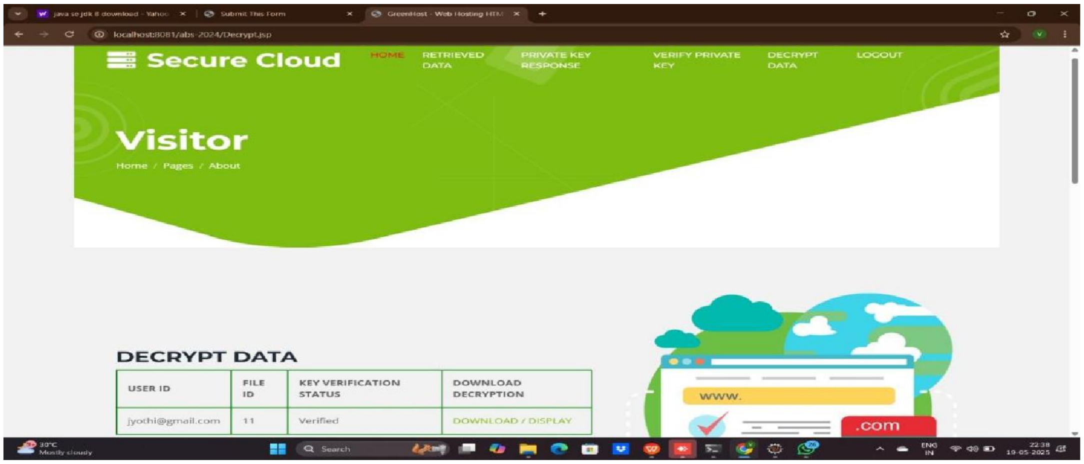
Login Reset

EXPLANATION:

The image displays a web titled "Secure Cloud" with "Data Owner" as the main section. The current page is "Store Cloud Data," and it presents a form for uploading files.

DOI: 10.48175/IJARSCT-27701

Decrypted Data



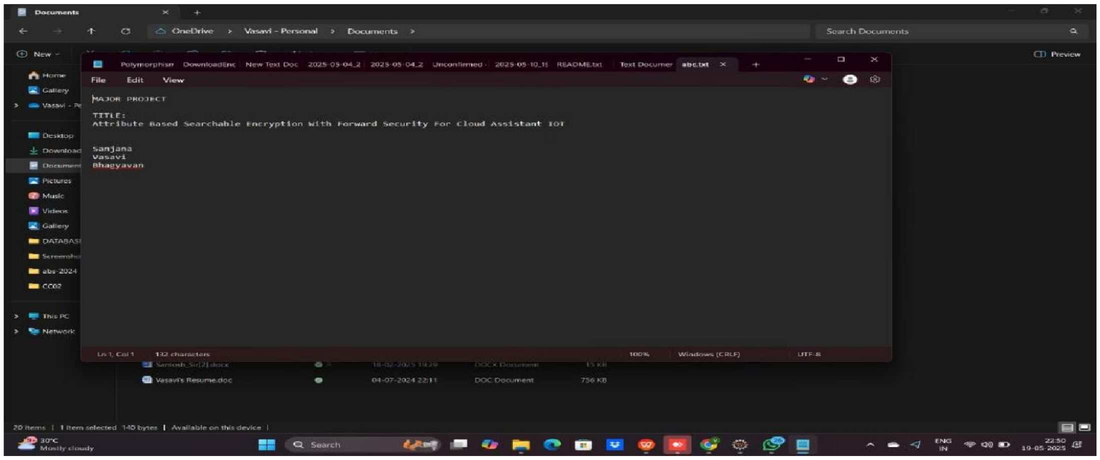
DECRYPT DATA

USER ID	FILE ID	KEY VERIFICATION STATUS	DOWNLOAD DECRYPTION
jyothi@gmail.com	11	Verified	DOWNLOAD / DISPLAY

EXPLANATION:

This page provides the interface for the visitor ("Jyothi") to finally access their data after successfully completing the private key generation and verification steps. The "Key Verification Status" being "Verified" confirms that the preceding security checks have passed.

Decrypted Data



```
MAJOR PROJECT

TITLE:
Attribute Based Searchable Encryption With Forward Security For Cloud Assistant IOT


Sanjana
Vasavi
Bhagyavan
```

VII. CONCLUSION

In this project we have introduced an advanced self-controlled data deletion scheme within a searchable mechanism. This scheme empowers DOs to effectively and permanently delete the ciphertext by puncturing their trapdoors with specific labels corresponding to the ciphertext. The data deletion process does not relay to trusted third parties, which will not generate additional communication overhead, and the data deletion process ensures forward security.The proposed system ensures that only users with the required attributes and satisfying specific contextual conditions can decrypt and search sensitive data stored in the cloud. This mitigates the risk of unauthorized access, especially in large-scale IoT deployments where traditional access control methods may fall short.

DOI: 10.48175/IJARSCT-27701

FUTURE ENHANCEMENT

Therefore, we give the algorithm constructions of the Pun-CP-ABSE scheme. The Pun-CP-ABSE scheme achieves fine-grained access control over encrypted data with a keyword search that enables the DO to retrieve the data corresponding to the keywords if the DO attribute can satisfy the access strategy. Moreover, we prove our scheme is secure against the CPA and CKA. Last, We implemented simulations of the Pun-CPABSE scheme to show its efficiency and practicability.In the future, the proposed context-aware secure search system can be enhanced in several ways to better suit the evolving needs of IoT cloud platforms. One key improvement would be enabling real-time context updates, allowing the system to adapt access control decisions based on dynamic environmental or user change.

REFERENCES

[1] S. Das and S. Namasudra, ‘‘Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure,’’ IEEE Trans. Ind.Informat., vol. 19, no. 1, pp. 821–829, Jan. 2024.

[2] Y. Wan, X. Lin, K. Xu, F. Wang, and G. Xue, ‘‘Extracting spatial linformation of IoT device events for smart home safety monitoring,’’ inProc. IEEE INFOCOM Conf. Comput. Commun., May 2024, pp. 1–10.

[3] Y. Miao, F. Li, X. Li, J. Ning, H. Li, K. R. Choo, and R. H.Deng, ‘‘Verifiable outsourced attribute-based encryption scheme for cloud-assisted mobile e-health system,’’ IEEE Trans. Dependable Secure Comput., early access, Jul. 4, 2024, doi: 10.1109/TDSC.2023.3292129.

[4] D. Ghopur, J. Ma, X. Ma, Y. Miao, J. Hao, and T. Jiang, ‘‘Puncturable ciphertext-policy attribute-based encryption scheme for efficient and flexible user revocation,’’ Sci. China Inf. Sci., vol. 66, no. 7, Jul. 2024,Art. no. 172104.

[5] X. Feng, J. Ma, S. Liu, Y. Miao, X. Liu, and K. R. Choo, ‘‘Transparent ciphertext retrieval system supporting integration of encrypted heterogeneous database in cloud-assisted IoT,’’ IEEE Internet Things J., vol. 9,no. 5, pp. 3784–3798, Mar. 2023.

[6] T. Liu, Y. Miao, K. R. Choo, H. Li, X. Liu, X. Meng, and R. H. Deng,‘‘Time-controlled hierarchical multikeyword search over encrypted datain cloud-assisted IoT,’’ IEEE Internet Things J., vol. 9, no. 13,pp. 11017–11029, Jul. 2022.

[7] D. X. Song, D. Wagner, and A. Perrig, ‘‘Practical techniques for searcheson encrypted data,’’ in Proc. IEEE Symp. Secur. Privacy., May 2000,pp. 44–55.

[8] F. Li, J. Ma, Y. Miao, X. Liu, J. Ning, and R. H. Deng, ‘‘A survey on searchable symmetric encryption,’’ ACM Comput. Surv., vol. 56, no. 5,pp. 1–42, May 2024.

[9] Z. Li, J. Ma, Y. Miao, X. Liu, and K.-K.-R. Choo, ‘‘Forward and backward secure keyword search with flexible keyword shielding,’’ Inf. Sci., vol. 576,pp. 507–521, Oct. 2021.

[10] Y. Miao, R. H. Deng, K. R. Choo, X. Liu, J. Ning, and H. Li, ‘‘Optimized verifiable fine-grained keyword search in dynamic multi-owner settings,’’ IEEE Trans. Dependable Secure Comput., vol. 18, no. 4, pp. 1804–1820,Jul. 2021.

[11] X. Li, H. Wang, S. Ma, M. Xiao, and Q. Huang, “Revocable and verifiable weighted attribute-based encryption with collaborative access for electronic health record in cloud,” Cybersecurity, vol. 7, no. 1, p. 18, Mar. 2021..

[12] H. Guo, W. Li, M. Nejad, and C.-C. Shen, “A hybrid blockchain-edge architecture for electronic health records management with attribute-based cryptographic mechanisms,” arXiv preprint arXiv:2305.19797, May 2021.

[13] S. Das and S. Namasudra, “Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure,” IEEE Transactions on Industrial Informatics, vol. 19, no. 1, pp. 821–829, Jan. 2020.

[14] J. Li, Y. Zhang, and T. Wang, “An efficient attribute-based encryption scheme with data security classification in the multi-cloud environment,” Electronics, vol. 12, no. 20, p. 4237, Oct. 2020.

[15] C. Ge, Z. Liu, W. Susilo, L. Fang, and H. Wang, “Attribute-based encryption with reliable outsourced decryption in cloud computing using smart contract,” IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 2, pp. 937–948, Mar.–Apr. 2018.

[16] X. Li, Y. Zhang, and J. Wang, “Blockchain-based and multi-authority hierarchical access control data sharing scheme,” Computers & Electrical Engineering, vol. 114, p. 109547, Jan. 2018.

DOI: 10.48175/IJARSCT-27701