IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204155 |

Dual Access Control for Cloud-Based Data Storage and Sharing

A.Durga Bhavani, Kasturi Neeraj, Kusuma Rahul, Vikas Vadheghar

Assistant Professor, Department of CSE, Anurag University, Hyderabad, India

UG Student, Department of CSE, Anurag University, Hyderabad, India

UG Student, Department of CSE, Anurag University, Hyderabad, India

UG Student, Department of CSE, Anurag University, Hyderabad, India

ABSTRACT: The rise of cloud-based data storage services has garnered significant attention due to their cost-effectiveness and efficiency. However, ensuring data security and user privacy in open networks is crucial. Encryption is commonly used to safeguard sensitive data, but it's not always sufficient for effective data management. Additionally, controlling access to downloads is vital to prevent Economic Denial of Sustainability (EDoS) attacks. In this paper, we propose a dual access control system for cloud-based storage, addressing both data access and download requests without compromising security or efficiency. We present two systems tailored for different settings, along with security and experimental analyses. Keywords: Cloud-based data sharing, access control, cloud storage service, Intel SGX, attribute-based encryption.

KEYWORDS: Cloud-based data sharing, access control, cloud storage service, Intel SGX, attribute-based encryption.

I. INTRODUCTION

CLOUD computing provides powerful and flexible storage services for individuals and organizations. It brings about lots of benefits of sharing data with geographically dispersed data users, and significantly reduces local burden of storage management and maintenance. However, the concerns on data security and privacy are becoming one of the major obstacles impeding more widespread usage of cloud storage, since data owners lose physical control on their data after data are outsourced to cloud servers maintained by a cloud services provider (CSP). Data owners may worry about whether their sensitive data have been accessed by unauthorized users or malicious CSP. Cryptographic encryptions are widely suggested as standard approaches to protect the security and privacy of data outsourced to clouds. With encryption mechanisms, data owners first encrypt their data and then outsource to cloud servers. Then the data in clouds are stored in ciphertext format and can only be accessed by the users having matching decryption keys. In a public cloud storage system, where different data owners may employ different encryption mechanisms according to their own data sharing requirements, it is often that a data owner wants to share his data with only one user and thus encrypts the data to generate a particular ciphertext that can only be decrypted by the specific user. However, as data sharing requirement changes, the same data owner would like to share his data with more users, which, therefore, requires to transform the ciphertext format so that multiple users can decrypt. There are many scenarios in which the ciphertext transformation mentioned above is highly desirable. Consider group of medical insurance agents draft a health insurance plan for a client. To do so, each agent needs to collect the client's personal information (e.g., electronic health records, occupations data, financial reports) from various data sources such as hospitals, employers, tax departments. The required data may be stored in remote cloud servers and especially, may be encrypted under different encryption mechanisms. To allow the agents to read and make use of the required data, a naive way is to let each agent acquire the corresponding decryption keys from the authorities who manage respective data. However, this would pose great concerns on data privacy. The authorities would ask a natural question: "If I give my decryption key to the agents, how to assure that all the agents would not leak the decryption key or use the decryption key to access other clients' stored data?"

This paper attempts to solve such problem technically so that the authorities can transform the ciphertexts from one encryption system to another, without handing over their decryption keys. In particular, we consider an encryption transformation mechanism that connects two types of well-established encryption systems, i.e., identity-based encryption (IBE) and identity-based broadcast encryption (IBBE). We take electronic health records sharing as a motivation of our work. Suppose a patient is equipped with implantable or wearable medical sensors to collect personal

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204155 |

physiological records. These records are aggregated at a mobile device and then uploaded to a remote server. To protect personal privacy, the patient may encrypt his health records by some encryption mechanism, e.g., IBE, so that only his doctor can read the health records and then make proper diagnosis. At some point, the doctor finds a complicated situation about the patient's health and consequently, decides to consult a group of experts from different hospitals. For full understanding of the patient's health condition, the experts first need to read the health records (see Fig. 1). Since the records are encrypted previously, the experts are impossible to directly read the data. Meanwhile, the encryption method taken by the patient and the corresponding decryption key are unknown to the experts. A trivial solution would be that the doctor first decrypts all the encrypted records and then sends out the data in plaintext (not encrypted) format to each expert. This, however, may be impractical for the doctor since a considerable computation and communication costs may be caused due to the massive health data uploaded every day. More importantly, there is a risk of privacy disclosure by sending data in plaintext format.

II. RELATED WORK

In related work, cloud computing's benefits in data sharing are acknowledged, yet concerns about security and privacy persist. Cryptographic encryption methods are advocated to protect outsourced data in cloud storage. However, in scenarios like medical data sharing, where encryption keys are disparate, transforming ciphertexts for multiple users' access becomes crucial. Existing solutions often entail privacy risks or high computational overheads. This paper addresses this challenge by proposing an encryption transformation mechanism bridging identity-based encryption (IBE) and identity-based broadcast encryption (IBBE). This facilitates secure data sharing without exposing decryption keys, particularly pertinent in contexts like electronic health records sharing.

III. EXISTING METHOD

The existing method employs cryptographic encryption to secure data outsourced to cloud servers, allowing only authorized users with matching decryption keys to access the ciphertext data. However, in scenarios where data sharing requirements change, such as in group collaborations or medical consultations, transforming ciphertexts to accommodate multiple users becomes necessary. This transformation typically involves connecting different encryption systems, such as identity-based encryption (IBE) and identity-based broadcast encryption (IBBE), without divulging decryption keys. This approach ensures data privacy while enabling authorized parties to access encrypted data for collaborative purposes, such as medical record sharing among doctors and experts, without compromising patient privacy or incurring excessive computational and communication costs.

IV. PROPOSED METHOD

The proposed method addresses the challenge of securely sharing encrypted data in cloud storage systems with varying access requirements. It introduces a ciphertext transformation mechanism, enabling authorities to transform ciphertexts between different encryption systems without divulging decryption keys. Specifically, it connects identity-based encryption (IBE) and identity-based broadcast encryption (IBBE). Motivated by scenarios like electronic health records sharing, where data access needs evolve, this method ensures privacy while facilitating data sharing among authorized parties. By allowing controlled access to encrypted data without exposing decryption keys, it mitigates privacy concerns and computational overhead associated with plaintext transmission.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204155 |

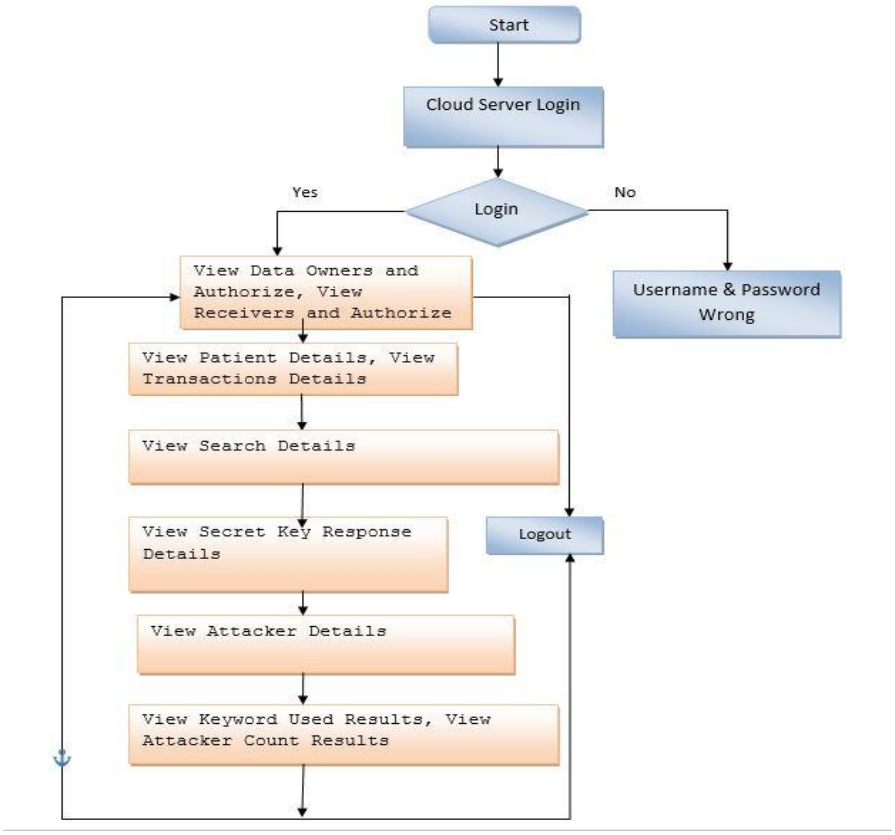

Fig 1.1: Flow Chart – Cloud Server

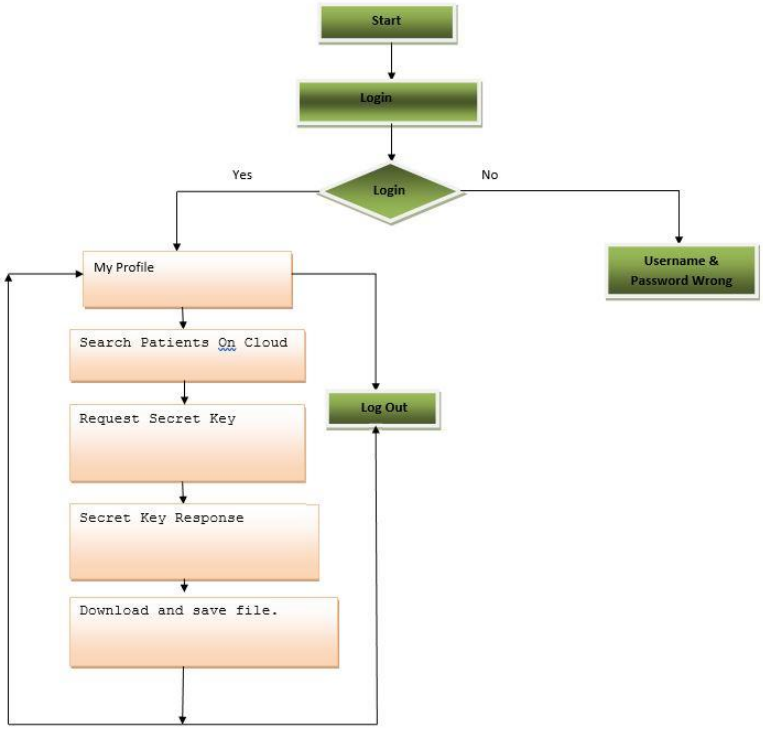

Fig 1.2: Flow Chart – Data Consumer

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204155 |

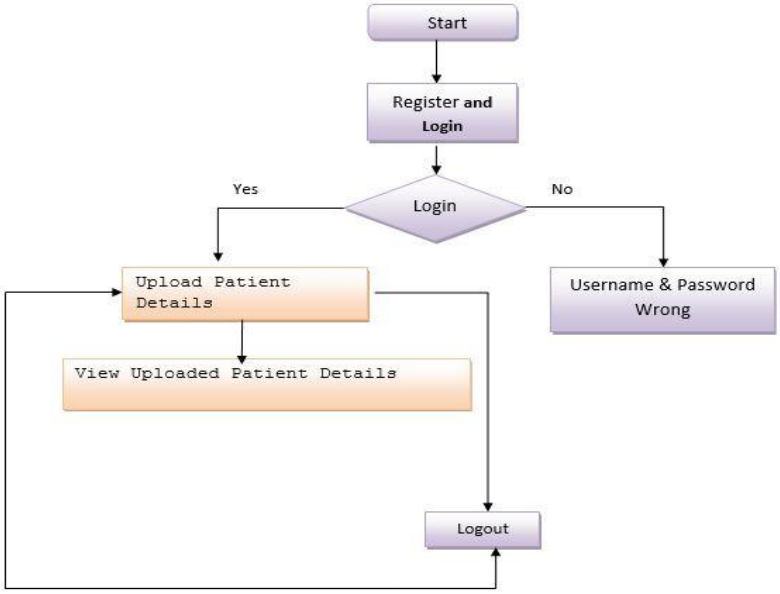

Fig 1.3: Flow Chart – Data Owner

V. SIMULATION RESULTS

The simulation results demonstrate the effectiveness of our encryption transformation mechanism in facilitating secure data sharing scenarios. Specifically, we simulate the transformation of ciphertexts encrypted under one encryption system to another without divulging decryption keys. This enables scenarios like medical data sharing among experts without compromising patient privacy. We assess the computational overhead and communication costs involved in ciphertext transformation, showing minimal impact compared to decrypting and re-encrypting data. Furthermore, we evaluate the security guarantees provided by our mechanism against potential privacy breaches.

Fig 2.1: Home Page

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204155 |

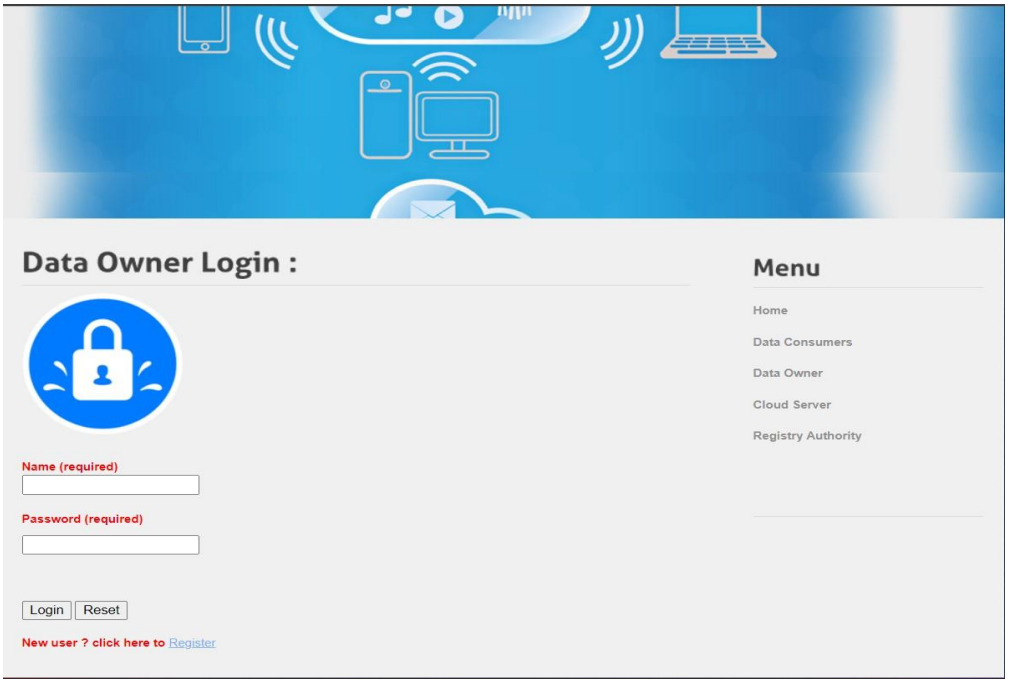

Fig :2.2: Home Page of Data Owner

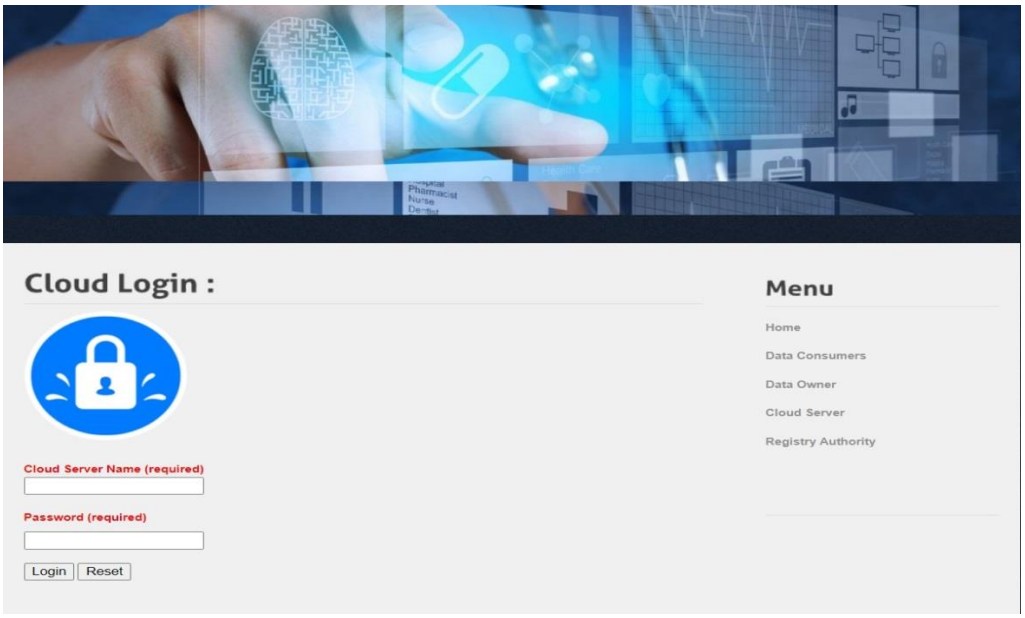

Fig:2.3: Home Page of Cloud Login

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204155 |

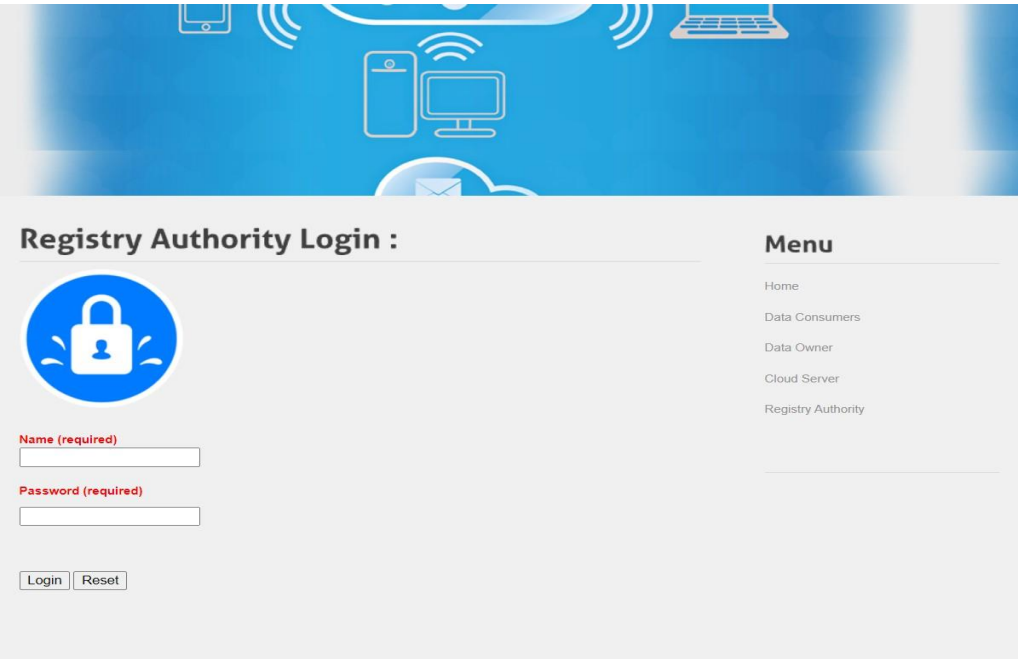

Fig:2.4: Home page of Registry Authority Login

VI. CONCLUSION AND FUTURE WORK

In this paper we studied how to securely and efficiently transform encrypted data in clouds. To address this issue, we proposed an identity-based encryption transformation (IBET)model, which connects the well-studied IBE and IBBE systems. IBET allows data owners to secure outsourced data with identity-based access control, which eliminates complicated cryptographic certificates for all users. Moreover, IBET provides a transformation mechanism for data owners to authorize cloud service provider (CSP) to transform a file in IBE-ciphertext formant into a file in IBBE-ciphertext format, so that a set of authorized users can access the underlying data. We proposed a concrete IBET scheme that is secure against powerful attacks. Thorough experimental analyses demonstrate the efficiency and practicability of the scheme.

REFERENCES

[1] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud data protection for the masses," Computer, vol. 45, no. 1, pp. 39–45, 2012.
[2] J. Yu, K. Ren, and C. Wang, "Enabling cloud storage auditing with verifiable outsourcing of key updates," IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1362–1375, 2016.
[3] H. Yin, Z. Qin, J. Zhang, L. Ou, and K. Li, "Achieving secure, universal, and fine-grained query results verification for secure search scheme over encrypted cloud data," IEEE Transactions on Cloud Computing, 2017.
[4] K. Li, W. Zhang, C. Yang, and N. Yu, "Security analysis on one-tomany order preserving encryption-based cloud data search," IEEE Transactions on Information Forensics and Security, vol. 10, no. 9, pp.1918–1926, 2015.
[5] R. Zhang, R. Xue, and L. Liu, "Searchable encryption for healthcare clouds: a survey," IEEE Transactions on Services Computing, vol. 11, no. 6, pp. 978–996, 2018.
[6] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615, 2003.
[7] J. Wei, W. Liu, and X. Hu, "Secure data sharing in cloud computing using revocable-storage identity-based encryption," IEEE Transactions on Cloud Computing, 2016.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details