Journal of Informatics
Electrical and Electronics Engineering, 2024,
Vol. 00, Iss. 00, S. No. 000, pp. 1-12
ISSN (Online): 2582-7006

Securely Cloud Data Storage and Sharing

Nishant kumar[1], Neelesh Jain[2], Prateek Singhal[3]

[1,2]Computer science & Engineering, SAM College of Engineering and Technology, Bhopal, India
[3]Department of Computer Engineering and Applications, GLA University, Mathura, India
[1]nraj6658@gmail.com, [3]prateeksinghal2031@gmai.com

How to cite this paper: N. Kumar, N. Jain and P. Singhal, "Securely Cloud Data Storage and Sharing," *Journal of Informatics Electrical and Electronics Engineering* (JIEEE).

Received: 05/09/2023
Accepted: 10/01/2024
Online First: 15/01/2024

Abstract

With the increasing adoption of cloud computing, data storage and sharing have become integral parts of our digital lives. However, ensuring the security and privacy of data stored in the cloud remains a significant challenge. This paper proposes a novel approach for securely storing and sharing data in the cloud, addressing the vulnerabilities associated with traditional cloud storage models. The proposed approach utilizes advanced cryptographic techniques, including hyperchaotic encryption and hash functions, to protect the confidentiality and integrity of data stored in the cloud. The hyperchaotic encryption algorithm provides a high level of security by introducing chaos-based dynamics into the encryption process, making it resistant to various attacks. Additionally, the hash function ensures the integrity of data by generating unique identifiers for each file stored in the cloud. To enhance data sharing security, the proposed approach employs access control mechanisms and user authentication protocols. Access control rules are enforced to restrict unauthorized access to data, while user authentication ensures that only legitimate users can access and modify the shared data.

Keywords

Cloud Computing, Data Sharing, Cloud data Storage, Efficient Data sharing

1. Introduction

In recent years, cloud computing has revolutionized the way we store, access, and share data. It provides convenient and cost-effective solutions for individuals and organizations to store their data in remote servers and access it from anywhere at any time. However, the growing dependence on cloud storage has raised concerns about the security and privacy of data. Traditional cloud storage models rely on the assumption that the cloud service provider is fully trusted, which may not always be the case. Unauthorized access, data breaches, and insider attacks pose significant threats to the confidentiality and integrity of stored data. Therefore, there is a pressing need for robust and secure solutions to protect sensitive information in the cloud. This paper focuses on addressing the challenges of securely storing and sharing data in the cloud. It proposes an innovative approach that combines advanced cryptographic techniques with access control mechanisms and user authentication protocols to ensure the security and privacy of cloud data.

The primary objective of this research is to develop a secure cloud data storage and sharing system that provides end-to-end protection for data at rest and in transit. The proposed approach leverages hyperchaotic encryption, a powerful encryption algorithm based on chaos theory, to enhance the confidentiality of stored data. By introducing chaos-based dynamics into the encryption process, hyperchaotic encryption offers a high level of security that is resistant to various attacks. In addition to encryption, this research also incorporates hash functions to ensure the integrity of stored data. Hash functions generate unique identifiers, or hashes, for each file stored in the cloud. These hashes serve as fingerprints for data integrity verification, allowing users to detect any unauthorized modifications or tampering of their files.

To control access to stored data, the proposed approach incorporates access control rules that define the permissions and restrictions for different users or user groups. This ensures that only authorized individuals can access, view, or modify specific data, safeguarding sensitive information from unauthorized disclosure or manipulation. Furthermore, user authentication protocols are implemented to verify the identities of users before granting them access to the cloud data. This helps prevent unauthorized users from accessing confidential data and ensures that only legitimate users can engage in data sharing and collaboration activities.

This paper will present the details of the proposed approach, including the underlying cryptographic techniques, access control mechanisms, and user authentication protocols. It will also discuss the implementation of the approach using a cloud storage platform and evaluate its performance, security, and usability.

2. Cloud Computing

Cloud computing is a paradigm that has revolutionized the way we store, process, and access data and applications. It involves the delivery of computing services, such as servers, storage, databases, networking, software, and analytics, over the internet. Instead of hosting these resources locally, organizations and individuals can utilize the vast infrastructure and capabilities of cloud service providers.

Cloud computing offers numerous benefits, including scalability, flexibility, cost-efficiency, and ease of management. Users can easily scale their resources up or down based on demand, paying only for the resources they consume. This eliminates the need for upfront investments in hardware and infrastructure, allowing businesses to focus on their core activities.

One of the key advantages of cloud computing is its ability to enable ubiquitous access to data and applications. Users can access their files, software, and services from any device with an internet connection, making remote work and collaboration more seamless. This flexibility promotes productivity and enhances business agility.

Cloud computing also provides robust data storage and backup solutions. Data is stored in distributed data centers, ensuring redundancy and data durability. This minimizes the risk of data loss and offers disaster recovery capabilities. Additionally, cloud providers often implement advanced security measures to protect data from unauthorized access, ensuring data privacy and compliance with regulations.

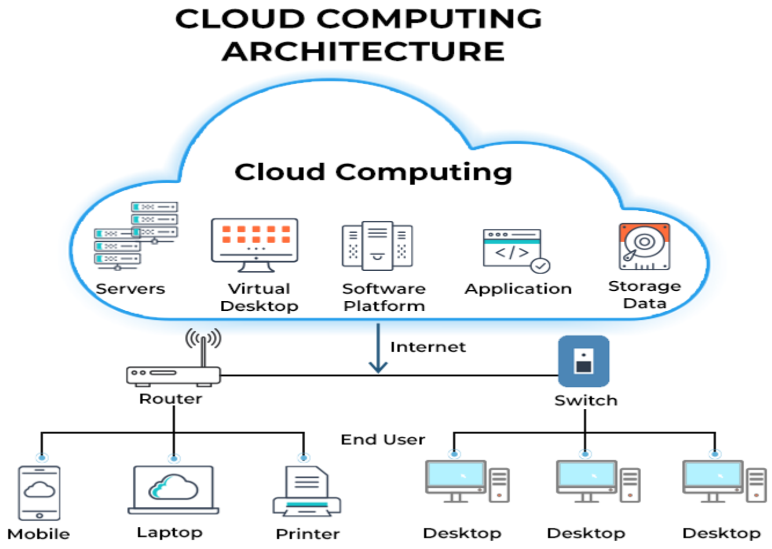


Figure 1. Cloud Computing Architecture

3. Proposed Method

In this proposed work the following techniques is used:

Data Encryption:

a. Choose a suitable hyperchaotic system, such as the Lorenz system or the Chua circuit, and implement it in Java.

b. Implement key generation algorithms for generating encryption keys based on the hyperchaotic system.

c. Develop an encryption algorithm that takes the hyperchaotic system parameters and the encryption key as inputs and performs encryption on the data blocks.

d. Use symmetric encryption algorithms (e.g., AES) along with hyperchaotic encryption to enhance security.

e. Encrypt the data blocks using the encryption algorithm and store them as encrypted files.

Hash Function:

a. Choose a secure hash function, such as SHA-256 or SHA-3, and use Java's built-in cryptographic libraries (e.g., MessageDigest) to implement it.

b. Define a function that takes a data block as input and returns its hash value.

c. Compute the hash value for each data block using the implemented hash function.

Cloud Storage:

a. Set up an account with a cloud storage provider (e.g., Amazon S3, Google Cloud Storage).

b. Use Java's cloud storage APIs or SDKs provided by the provider to establish a secure connection and authenticate with the cloud storage service.

c. Split the encrypted data into smaller blocks or chunks for efficient storage and retrieval.

d. Upload the encrypted data blocks to the cloud storage provider, ensuring data integrity by computing and storing the

corresponding hash values for each block.
e. Store the mapping between the data blocks and their respective locations in cloud storage.

Data Sharing:
a. Implement user authentication and authorization mechanisms to validate user access to the shared data.
b. Develop secure methods for users to share encrypted data with other authorized users, such as generating and sharing encryption keys securely.
c. Consider implementing access control mechanisms, such as role-based access control, to regulate data sharing among authorized users.
d. Ensure that encryption keys are securely shared only with authorized users.

Data Retrieval:
a. Retrieve the encrypted data blocks from the cloud storage provider based on user requests.
b. Verify the integrity of the retrieved data blocks by recomputing their hash values and comparing them with the stored hash values.
c. Decrypt the data blocks using the encryption algorithm and the appropriate decryption keys.
d. Reassemble the decrypted data blocks to reconstruct the original data.

Key Management:
a. Develop secure key generation algorithms to generate encryption keys for users.
b. Implement mechanisms for securely distributing and storing encryption keys, such as using asymmetric encryption and secure key storage solutions.
c. Consider implementing key revocation mechanisms to handle scenarios where a user's access needs to be revoked.

Security Measures:
a. Implement secure communication protocols, such as HTTPS, for transmitting data between the client and the cloud storage provider.
b. Apply encryption to data both in transit and at rest to protect against unauthorized access or data breaches.
c. Regularly update and patch software components to address any security vulnerabilities.
d. Follow best practices for secure coding, such as input validation and output encoding, to prevent common security issues like injection attacks.

Testing and Evaluation:
a. Conduct comprehensive testing to ensure the correctness and robustness of the implemented system.
b. Evaluate the security features of the system, including encryption strength, key management, and access control mechanisms.
c. Measure the performance and scalability of the system under different workloads and evaluate its efficiency in handling data storage and sharing operations.

4. Result

This work implements a secure data storage and sharing method on the Java platform, specifically designed for cloud servers. The proposed method utilizes a combination of hyperchaotic encryption and hash functions to ensure the security of the stored data. Through simulations, we demonstrate the effectiveness of the proposed method in protecting data in a cloud server environment. The simulation outputs showcase the encryption process using hyperchaotic algorithms and the utilization of hash functions to enhance data security.

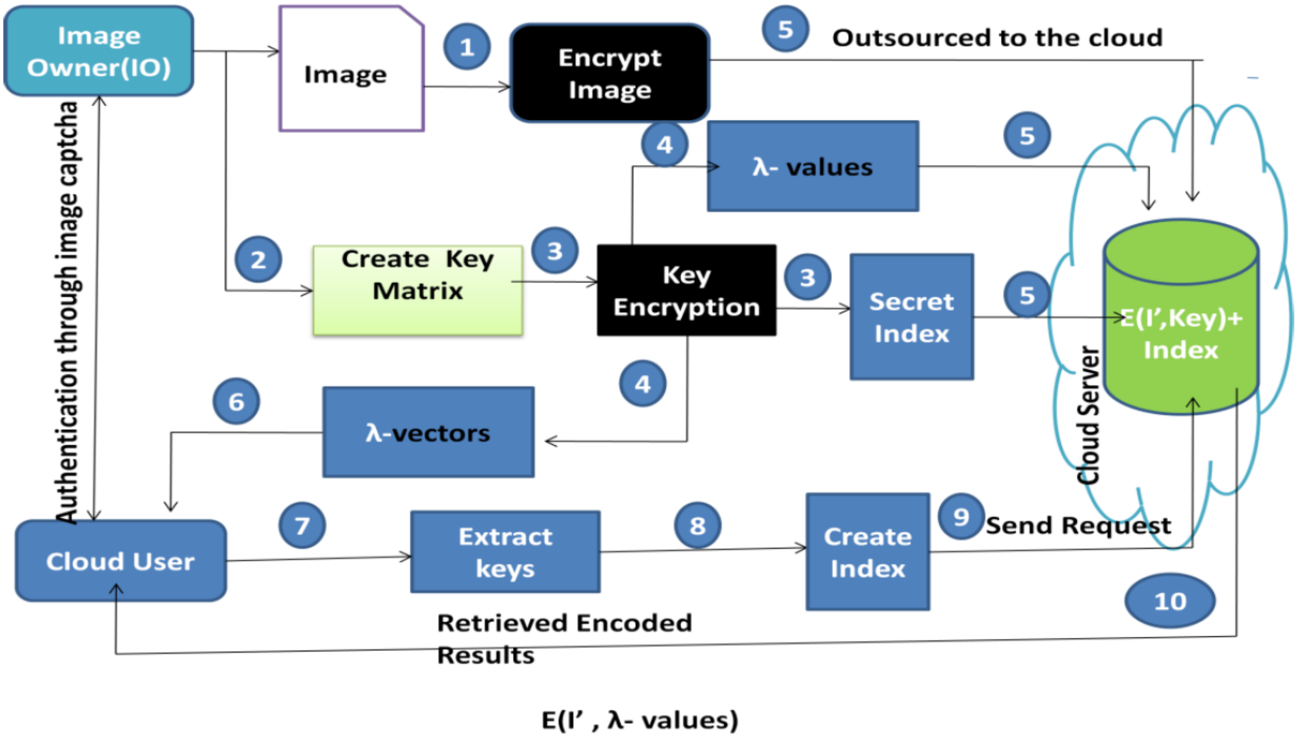


Figure 2. System framework

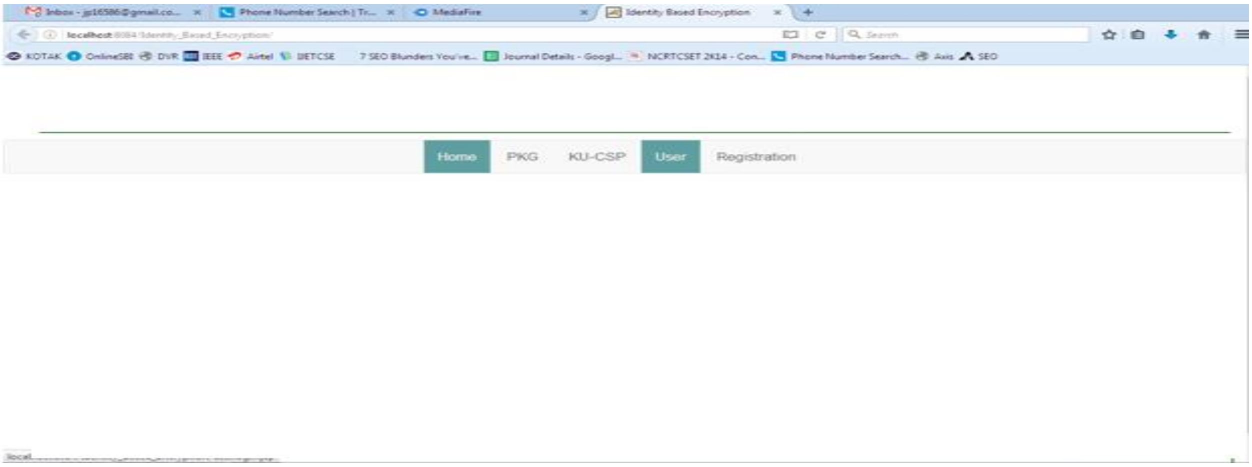


Figure 3. Home page of proposed work

In figure 3, the home page of the application features a user-friendly interface with various menus, including PKG, KU-CSP, User, and Registration. The main section of the home page displays the title of the application along with a brief summary of the abstract. Users can access the registration and login pages directly from this home page, allowing them to create an account or sign into their existing account. The purpose of this page is to provide an overview of the application and allow users to easily navigate to the desired sections.

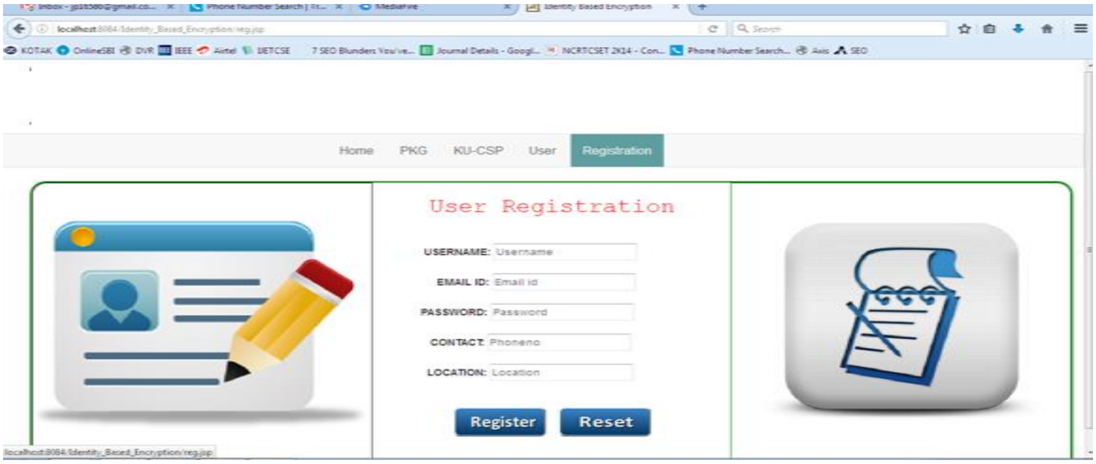


Figure 4. Registration page for user

Fig.4 The user registration page is designed to collect necessary information from the user. On this page, users are prompted to enter their username, email address, contact number, location, and password. Once all the required details are provided, the user can proceed to register by clicking the registration button. Upon successful registration, the user will be able to log in to their account using the provided credentials. The registration page ensures that users can easily create an account and gain access to the application's features and functionalities.

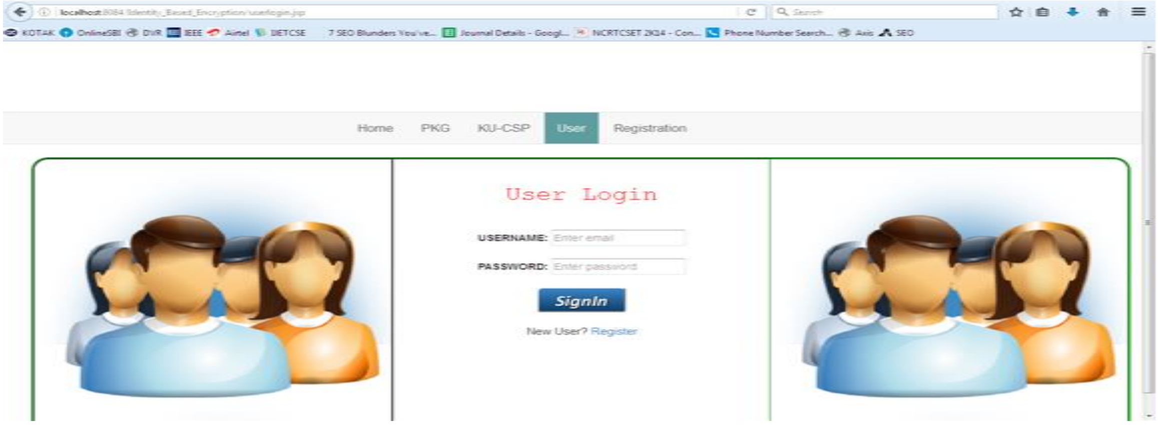
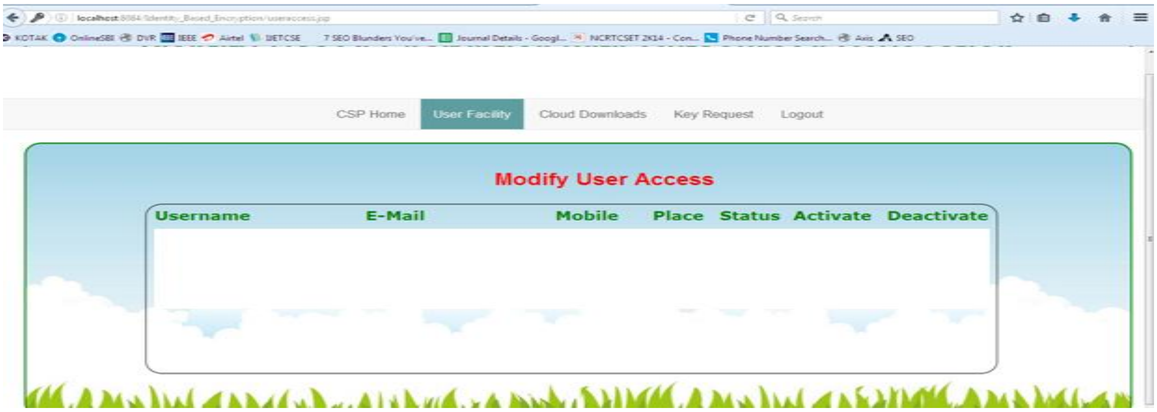


Figure 5. Login page for user

Fig.5. The user login page provides a secure gateway for registered users to access their accounts. On this page, users are required to enter their registered username and password. Once the correct credentials are provided, the user can proceed to log in by clicking the login button. Only users who have previously registered and have valid login credentials can access the panel. The login page ensures that only authorized users can gain entry to their respective accounts, maintaining the privacy and security of the system.

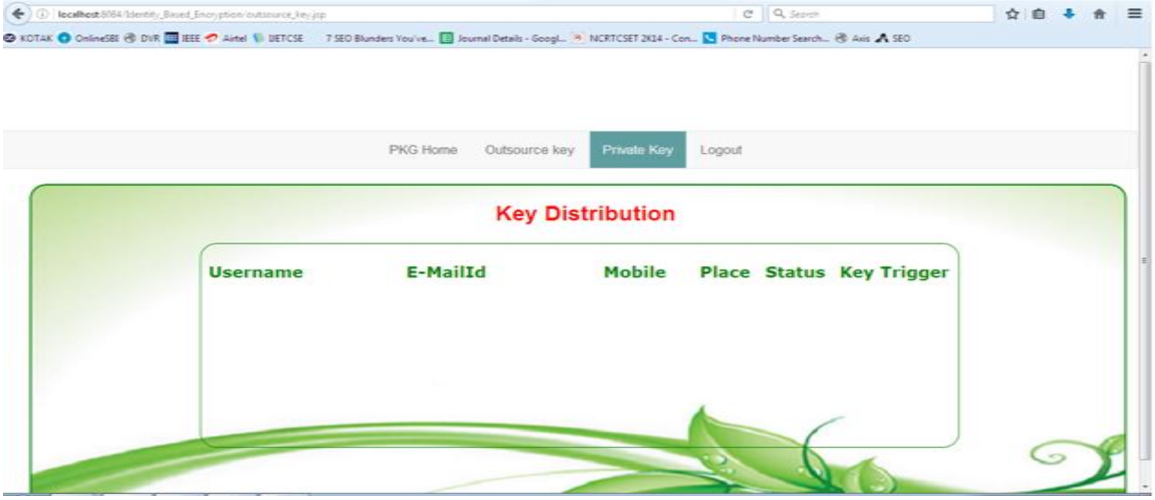


Modify User Access

Username	E-Mail	Mobile	Place	Status	Activate	Deactivate

Figure 6. User Panel

Fig.6 The user facility panel is a user-friendly interface that provides various features and functionalities to the activated users. Upon clicking the "Activate" button, the user gains access to the panel and can view its contents. The panel offers a range of options and tools that users can utilize to perform tasks, manage their account settings, and access the available resources. It serves as a centralized hub for users to navigate through different sections, interact with the system, and make use of the provided functionalities.

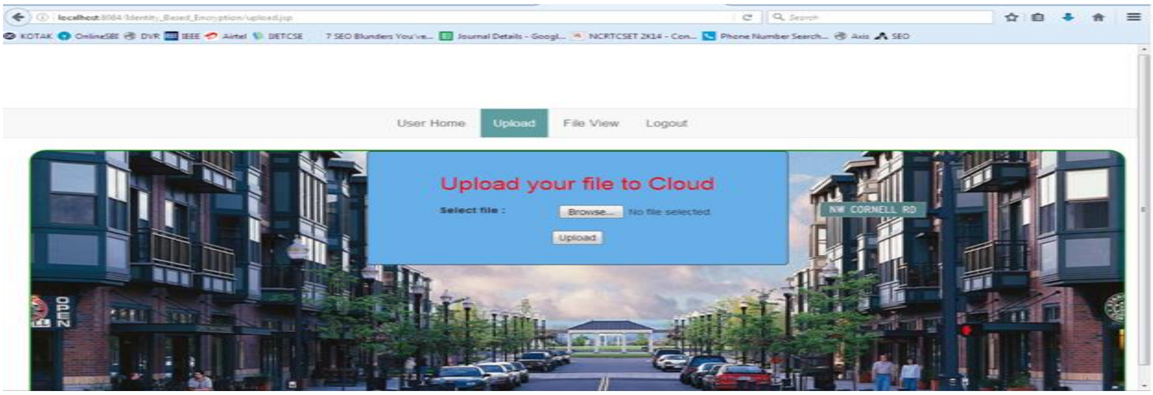


Key Distribution

Username	E-MailId	Mobile	Place	Status	Key Trigger

Figure 7. Key Distribution Section

Fig.7 The key distribution panel is a dedicated section that facilitates the distribution of keys to authorized users. Upon logging in, you will find a menu displaying options for private key and outsource key. To distribute the private key, navigate to the private key menu. Here, you can view the details of registered users, including their email addresses, mobile numbers, and status. This information allows you to efficiently manage and distribute the private keys to the intended recipients.

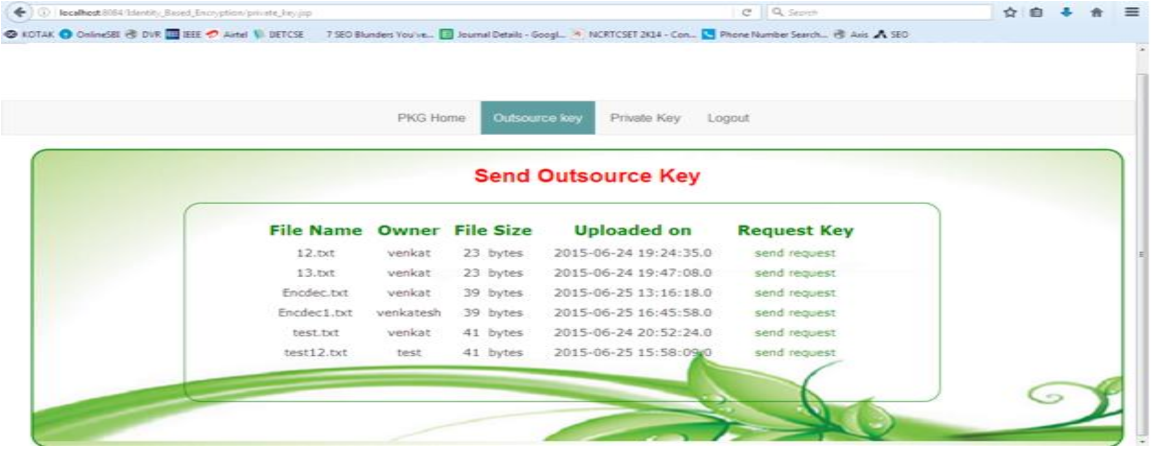


Upload your file to Cloud

Select file :

Figure 8. Data Upload to cloud server

Fig.8 The upload data feature allows users to securely upload their data files to the cloud server. By utilizing this functionality, users can easily transfer their files to the cloud for storage and sharing purposes. Simply select the desired data file from your local device and initiate the upload process. The system will securely transfer the file to the cloud server, ensuring the confidentiality and integrity of the data. Once the upload is complete, users can access and manage their uploaded files from the cloud server.



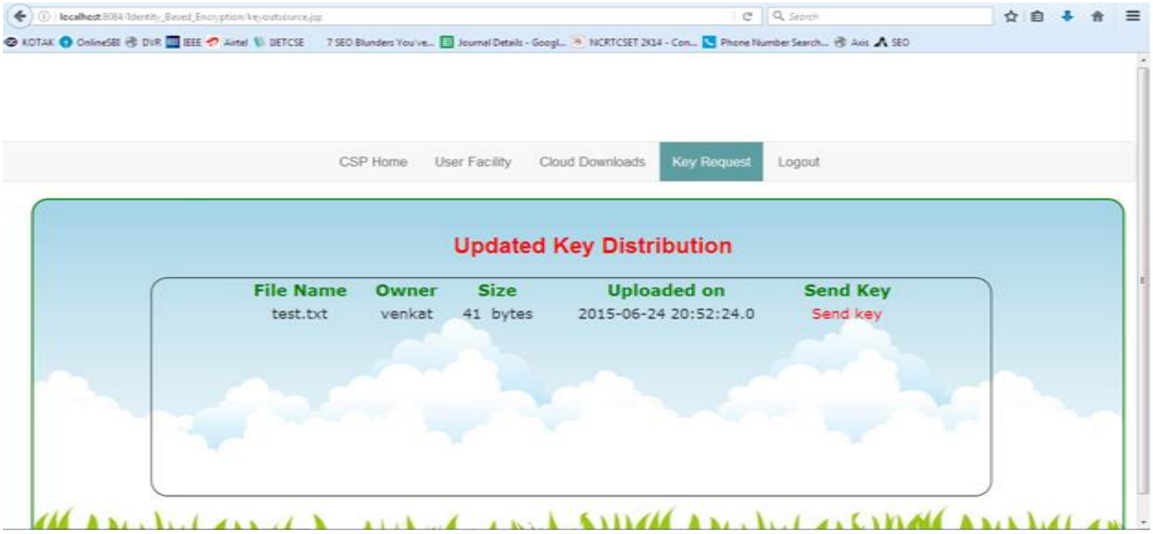
Send Outsource Key

File Name	Owner	File Size	Uploaded on	Request Key
12.txt	venkat	23 bytes	2015-06-24 19:24:35.0	send request
13.txt	venkat	23 bytes	2015-06-24 19:47:08.0	send request
Encdec.txt	venkat	39 bytes	2015-06-25 13:16:18.0	send request
Encdec1.txt	venkatesh	39 bytes	2015-06-25 16:45:58.0	send request
test.txt	venkat	41 bytes	2015-06-24 20:52:24.0	send request
test12.txt	test	41 bytes	2015-06-25 15:58:09.0	send request

Figure 9. Sending Key Panel

Fig 9 The Send Outsource Key panel facilitates the communication between the Private Key Generator (PKG) and the Cloud Service Provider (CSP). In this panel, the PKG can securely send the outsourced key to the CSP for storage and management. The process involves selecting the appropriate options and parameters for the key transfer, ensuring the confidentiality and

integrity of the outsourced key. Once the key transfer is initiated, the PKG securely transmits the key to the CSP, where it will be stored securely and made available for further operations and user access. This ensures the proper distribution and management of the outsourced key in the cloud environment.

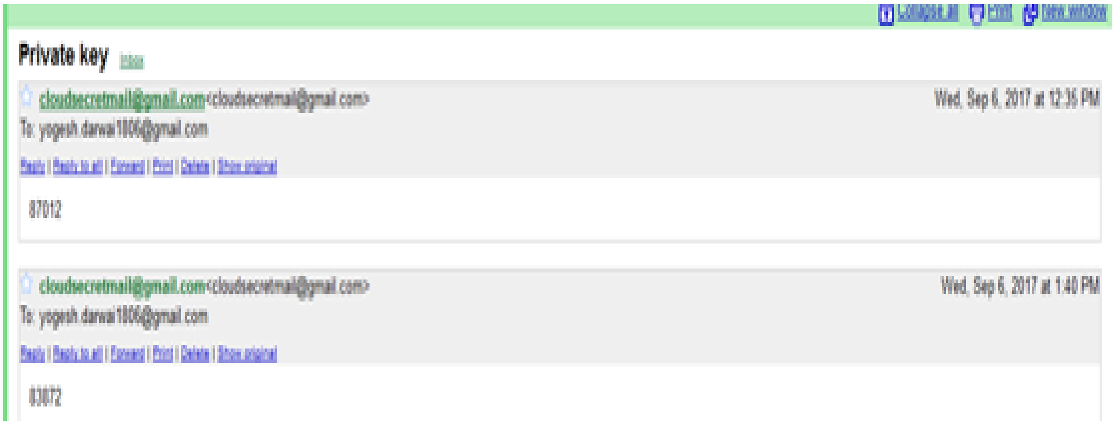


Updated Key Distribution

File Name	Owner	Size	Uploaded on	Send Key
test.txt	venkat	41 bytes	2015-06-24 20:52:24.0	Send key

Figure 10. Update key Distribution

Fig.10 Upon receiving the outsourced key from the Private Key Generator (PKG), the Cloud Service Provider (CSP) initiates the process to update the key for the users. The CSP verifies the trigger or request from the PKG and proceeds to generate the updated key based on the specified criteria or algorithm. Once the updated key is generated, the CSP securely sends it to the users' registered email addresses. This ensures that the users receive the latest key for accessing and managing their data securely in the cloud. The updated key is sent to the users' registered email addresses to maintain confidentiality and ensure that only authorized users have access to the key.


Collapse all
Print
New window

Private key

cloudsecretmail@gmail.com<cloudsecretmail@gmail.com> Wed, Sep 6, 2017 at 12:35 PM
To: yogesh.darwai1806@gmail.com

Reply | Reply to all | Forward | Print | Delete | Show original

87012

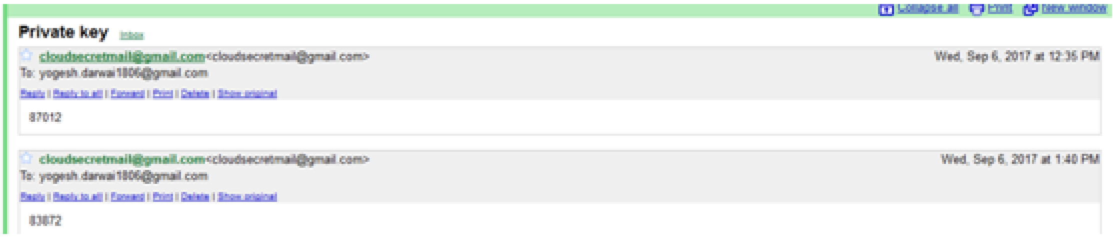
cloudsecretmail@gmail.com<cloudsecretmail@gmail.com> Wed, Sep 6, 2017 at 1:40 PM
To: yogesh.darwai1806@gmail.com

Reply | Reply to all | Forward | Print | Delete | Show original

83072

Figure 11. Private key in the mail

Fig.11 After the activation process, the private key is sent to the user's registered email ID. This private key serves as the final combined key required to access and view files stored in the cloud server. The user can download the files using the authorized key sent to their registered email ID. The authorized key ensures that only authorized users can download and access the files securely from the cloud server. By utilizing the respective authorized key received via email, the user can successfully download and retrieve their files from the cloud server.


Collapse all
Print
New window
Inbox
Reply | Reply to all | Forward | Print | Delete | Show original

Private key

cloudsecretmail@gmail.com<cloudsecretmail@gmail.com> Wed, Sep 6, 2017 at 12:35 PM
To: yogesh.darwai1806@gmail.com

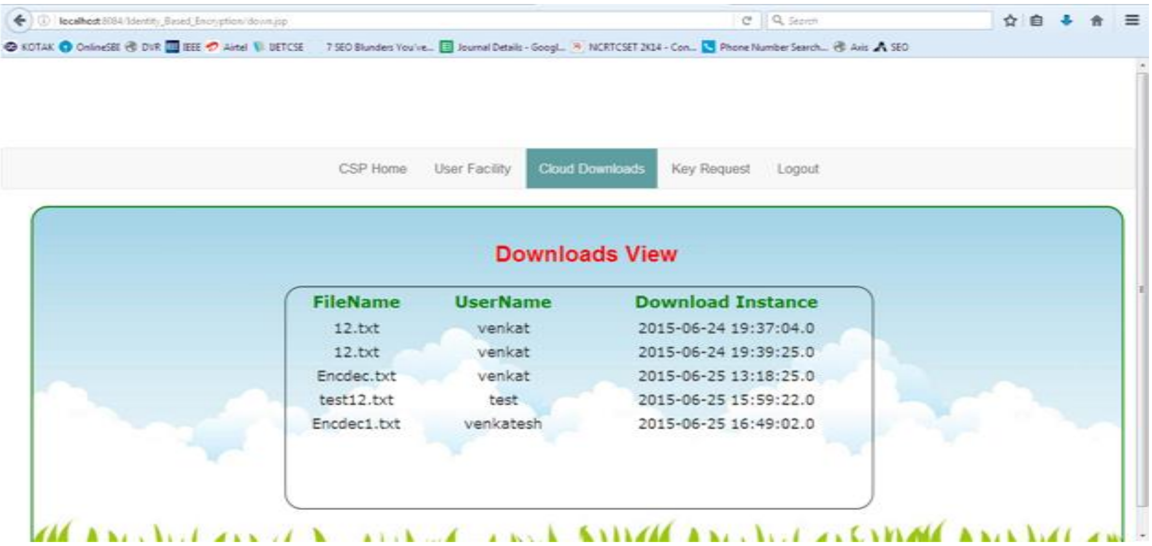
87012

cloudsecretmail@gmail.com<cloudsecretmail@gmail.com> Wed, Sep 6, 2017 at 1:40 PM
To: yogesh.darwai1806@gmail.com

83872

Figure 12. Permission key

This key refers to the file that is downloading as per the given key segment. This is known as provide key.



Downloads View

FileName	UserName	Download Instance
12.txt	venkat	2015-06-24 19:37:04.0
12.txt	venkat	2015-06-24 19:39:25.0
Encdec.txt	venkat	2015-06-25 13:18:25.0
test12.txt	test	2015-06-25 15:59:22.0
Encdec1.txt	venkatesh	2015-06-25 16:49:02.0

Figure 13. Cloud download view

Fig.20 shows download data in cloud server. After entering the provide key then shows the download view in the cloud server.

5. Conclusion

The increasing demand for data sharing has led to the widespread availability of Data Sharing and Collaboration in the Cloud. This chapter presents a comprehensive review of the utilization of Cloud computing technology to facilitate secure and confidential data sharing and collaboration. The authors explore various definitions related to Cloud computing and privacy, while also addressing the privacy and security concerns that impact the Cloud. Efforts to mitigate these issues are also discussed.

In this context, a proposed approach is introduced, which focuses on the development of a secure searchable image encryption method utilizing hyper chaos within a Cloud environment. This work extends an existing image security algorithm by incorporating two distinct phases. The first phase incorporates a well-established encryption technique for the initial level of security, while the second phase introduces a novel approach utilizing hyper chaos for both key and image encryption. Additionally, user authentication is implemented through image captcha, further enhancing the security of the system. By employing hyper chaos, the proposed method ensures the confidentiality of data and restricts access to authenticated users only. Notably, the system offers three layers of security, with two layers dedicated to authentication and one layer for encryption. Consequently, users are granted access to the encryption key only after successful authentication as recognized users.

References

[1]. P. Sharma, M. D. Borah, and S. Namasudra, "Improving security of medical big data by using Blockchain technology," Computers & Electrical Engineering, vol. 96, p. 107529, 2021.

[2]. T. P. Ezhilarasi, N. Sudheer Kumar, T. P. Latchoumi, and N. Balayesu, "A secure data sharing using IDSS CP-ABE in cloud storage," in Advances in Industrial Automation and Smart Manufacturing, Springer, Singapore, 2021, pp. 1073-1085.

[3]. Y. Chen, L. Meng, H. Zhou, and G. Xue, "A blockchain-based medical data sharing mechanism with attribute-based access control and privacy protection," Wireless Communications and Mobile Computing, 2021.

[4]. C. Ge, W. Susilo, J. Baek, Z. Liu, J. Xia, and L. Fang, "A verifiable and fair attribute-based proxy re-encryption scheme for data sharing in clouds," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 5, pp. 2907-2919, 2021.

[5]. R. Sivan and Z. A. Zukarnain, "Security and privacy in cloud-based e-health system," Symmetry, vol. 13, no. 5, p. 742, 2021.

[6]. N. Eltayieb, R. Elhabob, A. Hassan, and F. Li, "A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud," Journal of Systems Architecture, vol. 102, p. 101653, 2020.

[7]. P. Sun, "Security and privacy protection in cloud computing: Discussions and challenges," Journal of Network and Computer Applications, vol. 160, p. 102642, 2020.

[8]. C. Ge, W. Susilo, Z. Liu, J. Xia, P. Szalachowski, and L. Fang, "Secure keyword search and data sharing mechanism for cloud computing," IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 6, pp. 2787-2800, 2020.

[9]. T. Bhatia, A. K. Verma, and G. Sharma, "Towards a secure incremental proxy re-encryption for e-healthcare data sharing in mobile cloud computing," Concurrency and Computation: Practice and Experience, vol. 32, no. 5, p. e5520, 2020.

[10]. D. Zheng, B. Qin, Y. Li, and A. Tian, "Cloud-assisted attribute-based data sharing with efficient user revocation in the internet of things," IEEE Wireless Communications, vol. 27, no. 3, pp. 18-23, 2020.

[11]. H. Li, C. Lan, X. Fu, C. Wang, F. Li, and H. Guo, "A secure and lightweight fine-grained data sharing scheme for mobile cloud computing," Sensors, vol. 20, no. 17, p. 4720, 2020.

[12]. G. Elavarasan and S. Veni, "Data Sharing Attribute-Based Secure with Efficient Revocation in Cloud Computing," in 2020 International Conference on Computing and Information Technology (ICCIT-1441), IEEE, September 2020, pp. 1-6.

[13]. M. A. Islam and S. Madria, "Attribute-based encryption scheme for secure multi-group data sharing in cloud," IEEE Transactions on Services Computing, 2020.

[14]. N. Eltayieb, P. Wang, A. Hassan, R. Elhabob, and F. Li, "ASDS: Attribute-based secure data sharing scheme for reliable cloud environment," Security and Privacy, vol. 2, no. 2, p. e57, 2019.

[15]. S. Namasudra, "An improved attribute-based encryption technique towards data security in cloud computing," Concurrency and Computation: Practice and Experience, vol. 31, no. 3, p. e4364, 2019.

[16]. S. Han, K. Han, and S. Zhang, "A data sharing protocol to minimize security and privacy risks of cloud storage in big data era," IEEE Access, vol. 7, pp. 60290-60298, 2019.

[17]. S. Nalajala, K. Akhil, V. Sai, D. C. Shekhar, and P. Tumuluru, "Light weight secure data sharing scheme for mobile cloud computing," in 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), IEEE, December 2019, pp. 613-617.

[18]. J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," Computers & Security, vol. 72, pp. 1-12, 2018.

[19]. A. Wu, D. Zheng, Y. Zhang, and M. Yang, "Hidden policy attribute-based data sharing with direct revocation and keyword search in cloud computing," Sensors, vol. 18, no. 7, p. 2158, 2018.

[20]. Y. Zhang, A. Wu, and D. Zheng, "Efficient and privacy-aware attribute-based data sharing in mobile cloud computing," Journal of Ambient Intelligence and Humanized Computing, vol. 9, no. 4, pp. 1039-1048, 2018.

[21]. Q. Huang, W. Yue, Y. He, and Y. Yang, "Secure identity-based data sharing and profile matching for mobile healthcare social networks in cloud computing," IEEE Access, vol. 6, pp. 36584-36594, 2018.

[22]. M. Sookhak, F. R. Yu, M. K. Khan, Y. Xiang, and R. Buyya, "Attribute-based data access control in mobile cloud computing: Taxonomy and open issues," Future Generation Computer Systems, vol. 72, pp. 273-287, 2017.

[23]. A. Alotaibi, A. Barnawi, and M. Buhari, "Attribute-based secure data sharing with efficient revocation in fog computing," Journal of Information Security, vol. 8, no. 03, p. 203, 2017.

[24]. A. Sara, Y. Tassnim, and M. Abdellatif, "Secure confidential big data sharing in cloud computing using KP-ABE," in Proceedings of the 2nd international Conference on Big Data, Cloud and Applications, 2017, pp. 1-4.

[25]. N. S. B. Johari, "Improving Security and Efficiency In Attribute Based Data Sharing,"