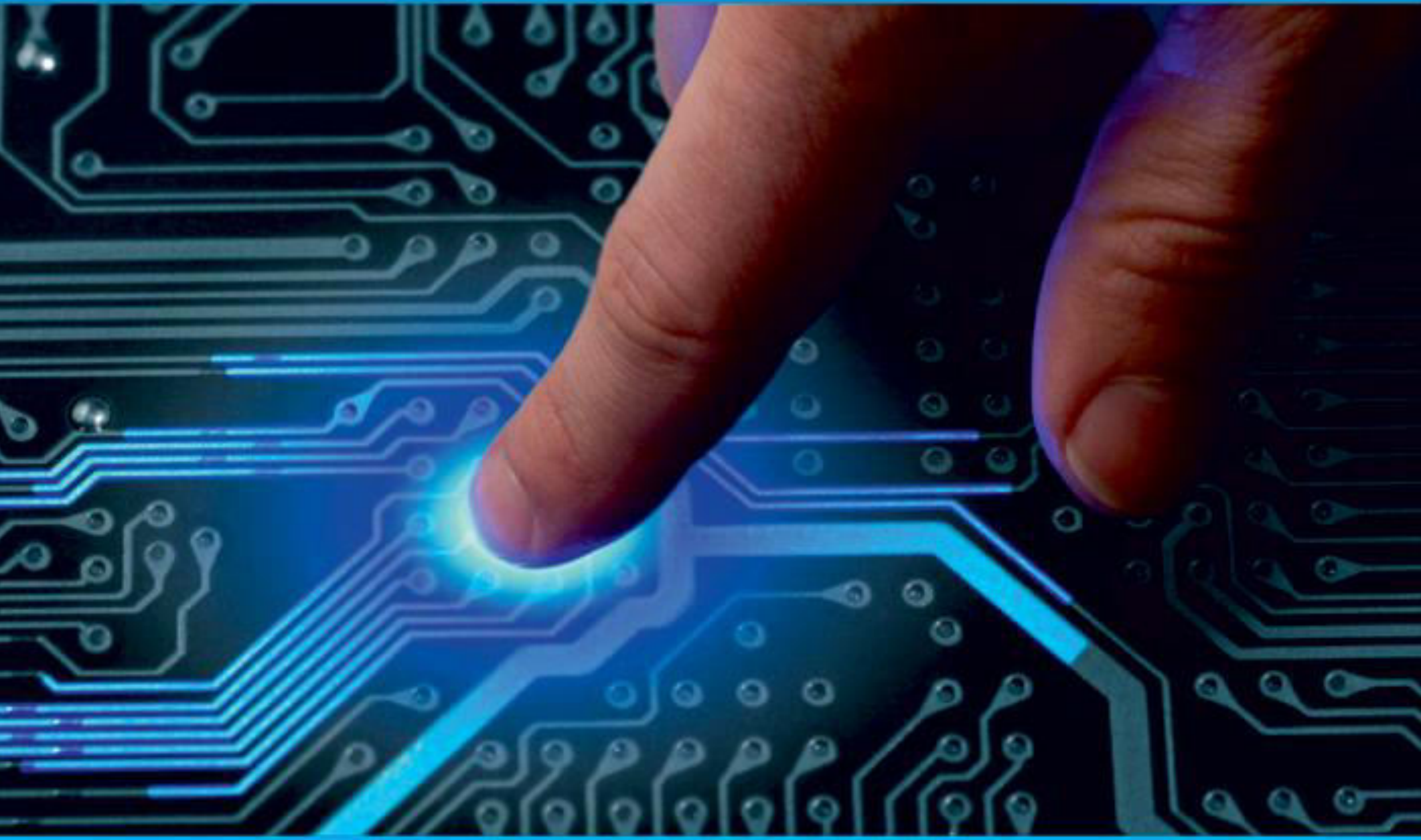
IJIRCCE

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



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 3, March 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

# Data Integrity Protection of Secret Data Sharing Through Algorithms

**B.V.V.H.Chandra Sekhar[1], P.Vamsi Krishna[2], Likhitha Bandlamudi[3], Devineni Bhargavi [4], CH.Sumanth chowdary[5]**

Assistant Professor, Department of Information Technology, Kallam Haranadhareddy Institute of Technology, Chowdavaram, Guntur (DT), Andhra Pradesh, India[1]

B.Tech Students, Department of Information Technology, Kallam Haranadhareddy Institute ofTechnology, Chowdavaram, Guntur(DT), Andhra Pradesh, India[2, 3, 4, 5]

**ABSTRACT:** Due to the least upfront capital investment, greatest scalability, and other advantages of the cloud environment, a significant number of academic institutions, government agencies, and business companies are adopting it. Despite the many features that the cloud environment supports, it also has many difficulties. In the context of information security and cloud computing, data protection is of utmost importance. To deal with this issue, many solutions have been created. It becomes necessary to research, classify, and analyse the significant existing work in order to investigate the applicability of these solutions to fulfil the requirements because there is a lack of thorough study among the current solutions. In-depth analysis of the top methods for secure sharing and data protection are presented in this article along with a comparative and systematic investigation.The discussion of each devoted technique covers its role in data protection, potential and ground-breaking solutions in the field, the essential and necessary information, such as workflow, achievements, scope, gaps, and future directions etc. for every solution. Furthermore, a complete and comparative examination of the discussed methodologies is offered. The relevance of the methodologies is then explored in relation to the needs, and the research gaps as well as potential future paths are reported. The authors hope that the contribution of this article will act as a stimulant for aspiring scholars to do research in the field.

## Objective

The main objective of this system is, SHA algorithm is used by the trusted authority to generate the key and that key will get share to user as well as the owner. The trusted authority module receives encrypted file using AES Algorithm from the data owner and computes hash value using MD-5 algorithm.

**KEYWORDS**: Cloud computing, data privacy and security, data protection, data storage, data sharing, IoT, machine learning, cryptography, watermarking, access control, differential privacy, probabilistic approaches.

## I. INTRODUCTION

One possible solution is to migrate character sequences to public cloud computing platforms and to request that Cloud Service Providers process sequence comparisons. At present, primary sequence comparison algorithms are deployed as a universal outsourcing service on public clouds. But at the same time, its security and privacy issues are increasingly emerging. The outsourced data stored as plaintext could easily be exposed to malicious external intruders and internal attackers in the CSP, and the individual private information carried by character sequences (e.g., personal identification, financial transaction records, genetic markers for some diseases, information that is used to identify paternity or maternity, etc.) could more or less be disclosed or abused. Therefore, secure outsourcing is designed to protect the privacy of character sequences, and to ensure that the scheduled computing requests are normally performed on the cloud servers.

For this purpose, we present a scheme called Encrypted Sequence Comparison based on a single-server model. Some novel salted hash and encryption techniques are employed to allow public clouds to perform sequence comparisons directly on the character sequences outsourced as cipher text. Overall, E-SC achieves a user-controlled reliable storage and a collusion-resistant outsourcing service, which plays an important role in the trade-off between security and execution performance. Our scheme is easy in deployment, efficient in processing and controllable in overhead. The contributions of this paper are mainly in the following four aspects.

Based on the universal model of a public cloud outsourcing, we propose an overall architecture for E-SC. This architecture is built on the end user and the unmodified CSP. Its overall system model, which has been demonstrated to be secure under the threat model, is user-friendly and implementation-friendly.

A salted hash algorithm is improved to hash the character sequences and the indexes of cost matrices, so as to defend against statistical attacks. An additive order preserving encryption algorithm is designed to encrypt the elements of cost matrices. Also, this algorithm can achieve an  in distinguish ability under additive ordered chosen-plaintext attack with linear time complexity.

A single cloud server works for the first time to provide a privacy-preserving computable outsourcing service to effectively resist collusion attacks from the cloud. With pre-processing modules of padding , partition ,and expansion, there is no need to decrypt any outsourced data in the non-interactive sequence comparison stage. 4) Simulation results show that the overall execution performance of our E-SC is negatively correlated with its security.

## II. RELATED WORK

**[1] A. K. Singh and I. Gupta, ''Online information leaker identification scheme for secure data sharing,'' Multimedia Tools Appl., vol. 79, no. 41, pp. 31165–31182, Nov. 2020.**

Due to the least upfront capital investment, greatest scalability, and other advantages of the cloud environment, a significant number of academic institutions, government agencies, and business companies are adopting it. Despite the many features that the cloud environment supports, it also has many difficulties. In the context of information security and cloud computing, data protection is of utmost importance. To deal with this issue, many solutions have been created. To investigate if these solutions may be applied to meet the requirements, it is necessary to study, classify, and assess the significant current work because the existing solutions lack complete analyses.The top methods for safely transferring and safeguarding data in a cloud environment are compared and analysed in-depth in this article. The following topics are covered in the explanation of each devoted technique: how it works to secure data, possibilities and cutting-edge solutions in the domain, the essential details about each solution, such as the workflow, accomplishments, scope, gaps, and future directions. A thorough and comparative study of the strategies covered is also provided.

**Summary:** Despite the many features that the cloud environment supports, it also has many difficulties. In the context of information security and cloud computing, data protection is of utmost importance.

**[2] E. Zaghloul, K. Zhou, and J. Ren, ''P-MOD: Secure privilege-based multilevel organizational data-sharing in cloud computing,'' IEEE Trans. Big Data, vol. 6, no. 4, pp. 804–815, Dec. 2020**

The way businesses store, access, and exchange data has changed as a result of cloud computing. Large data sets are continuously uploaded to the cloud and shared among a hierarchy of numerous people who have varying levels of access privileges. Finding a safe and effective data access structure has grown to be a significant research problem as more and more data storage requirements are shifting to the cloud. In order to manage and share massive data sets, a Privilege-based Multilevel Organizational Data-sharing system (P-MOD) that combines an attribute-based encryption method with an access structure based on privileges is described in this work.Our proposed privilege-based access structure helps reduce the complexity of designing hierarchies as the number of users grows, which enables managing healthcare records utilising mobile healthcare devices viable. Also, it can make it easier for businesses to use big data analytics to fully comprehend populations. If the DBDH assumption is true, security analysis demonstrates that P-MOD is secure against an adaptively chosen plaintext attack. P-MOD is more effective in terms of computational complexity and storage space than the previous schemes, as shown by the thorough performance and simulation evaluations utilising the real U.S. Census Income data set.

**Summary:** Large data sets are continuously uploaded to the cloud and shared among a hierarchy of numerous people who have varying levels of access privileges. Finding a safe and effective data access structure has grown to be a significant research problem as more and more data storage requirements are shifting to the cloud. In order to manage and share massive data sets, a Privilege-based Multilevel Organizational Data-sharing system (P-MOD) that combines an attribute-based encryption method with an access structure based on privileges is described in this work.

**[3] I. Gupta and A. K. Singh, ''GUIM-SMD: Guilty user identification model using summation matrix-based distribution,'' IET Inf. Secure., vol. 14, no. 6, pp. 773–782, Nov. 2020.**

To improve an enterprise's performance, data exchange among numerous entities is required. Yet, a hostile entity may disclose this information to an unauthorised third party, which might cause significant damage to the firms' finances, reputations, and long-term stability. In this paper, a novel approach called GUIM-SMD is presented for locating the guilty individual in a shared environment who leaked data to an unauthorised party. This model suggests an efficient distribution technique to distribute the data among the users based on the access control mechanism. The strategy introduces the summation matrix, which is calculated using the D- and U-scores that are given to the user and categorised data, respectively. Moreover, D-score and U-score have values between 0 and 1, and they depend on the relative data sensitivity and user guilt record. For data distribution among different users, the evaluated summation matrix is employed. In comparison to the previous work, the results reveal an improvement in average probability, average success rate, and detection rate of up to 98.74, 236.38, and 252.39%, respectively.

**Summary**: In this paper, a novel approach called GUIM-SMD is presented for locating the guilty individual in a shared environment who leaked data to an unauthorised party. This model suggests an efficient distribution technique to distribute the data among the users based on the access control mechanism. The strategy introduces the summation matrix, which is calculated using the D- and U-scores that are given to the user and categorised data, respectively.

**[4] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, ''Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage,'' IEEE Trans. Inf. Forensics Security, vol. 14, no. 2,pp. 331–346, Feb. 2019.**

Users can remotely store their data to the cloud and enable data sharing with others via cloud storage services. It is suggested to use remote data integrity auditing to ensure the reliability of cloud-stored data. The cloud file may contain certain sensitive information in some popular cloud storage systems, such as the electronic health records system. When the cloud file is shared, the sensitive information shouldn't be made available to others. The sensitive information can be realised by encrypting the entire shared file, but it will prevent others from using it. It has not yet been determined how to implement data sharing with sensitive information concealed in remote data integrity audits. To solve this issue, we offer a remote data integrity auditing system that enables data sharing with confidential information concealed in this essay. A sanitizer is employed in this method to turn the data blocks' signatures into valid ones for the sanitised file while also sanitising the data blocks that correspond to the file's sensitive information. During the integrity auditing process, these signatures are used to confirm the accuracy of the cleaned file. As a result, our method enables the cloud-stored file to be shared and utilised by others under the condition that the sensitive data is masked, while retaining the ability to effectively carry out remote data integrity auditing. The planned plan, however, is based on identity-based cryptography, which simplifies.

**Summary:** When the cloud file is shared, the sensitive information shouldn't be made available to others. The sensitive information can be realised by encrypting the entire shared file, but it will prevent others from using it. It has not yet been determined how to implement data sharing with sensitive information concealed in remote data integrity audits. To solve this issue, we offer a remote data integrity auditing system that enables data sharing with confidential information concealed in this essay.

**Existing Method:**Large-scale problems in the physical and life sciences are being revolutionized by Internet computing technologies, like grid computing, that make possible the massive cooperative sharing of computational power, bandwidth, storage, and data.

A weak computational device, once connected to such a grid, is no longer limited by its slow speed, small amounts of local storage, and limited bandwidth: It can avail itself of the abundance of these resources that is available elsewhere on the network. Without revealing to the remote agents whose computational power is being used, either one's data or the outcome of the computation on the data.

**Disadvantages**

- Secure outsourcing for widely applicable sequence comparison problems
- Risk of Leak of Secret Information

## III. PROPOSED SYSTEM

We propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group. We provide a secure way for key distribution without any secure communication channels. The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user.

Our scheme can achieve fine-grained access control, with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked.

We propose a secure data sharing scheme which can be protected from collusion attack. The revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud.

**Block Diagram:**

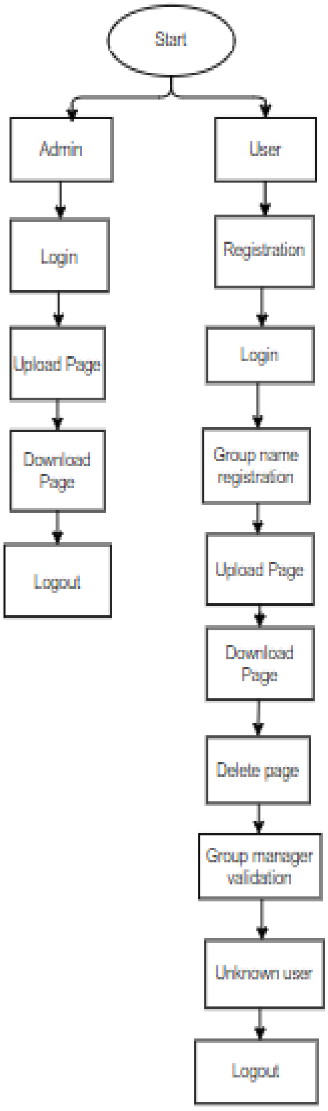
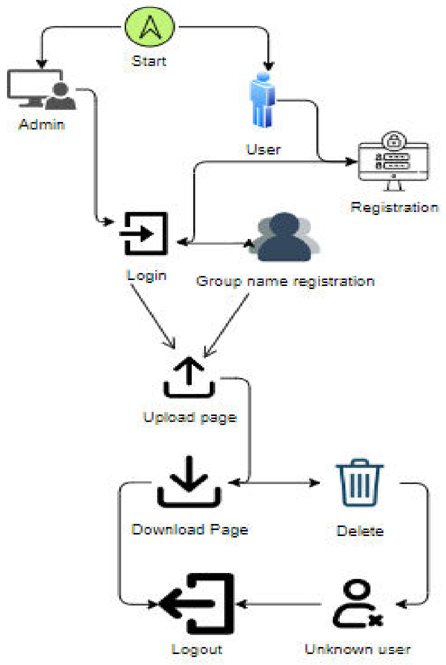


**Fig. Block diagram of proposed method**

**Architecture:**



**Advantages of proposed system:**

- Power Means of Persuasion and control
- More Reliable
- It's more secure and efficient.
- Data confidentiality

## IV. METHODOLOGY

### MD-5:

MD5 (Message-Digest Algorithm 5) is a widely used cryptographic hash function. It was invented by Ron Rivest in 1991 and was initially intended to be used as a way to verify the integrity of digital documents, such as emails or software. MD5 takes an input message of any length and produces a fixed-sized 128-bit hash value as output. The hash value is a unique digital fingerprint of the input message, which can be used to verify the authenticity and integrity of the message.

However, MD5 is now considered to be insecure for cryptographic purposes, as vulnerabilities have been found that can allow attackers to generate collisions (two different inputs that produce the same hash value). As a result, MD5 is no longer recommended for use in new applications, and other more secure hash functions such as SHA-256 or SHA-3 should be used instead.

### AES Algorithm:

AES (Advanced Encryption Standard) is a widely used symmetric-key encryption algorithm. It was selected by the National Institute of Standards and Technology (NIST) in 2001 as the standard encryption algorithm to replace the aging Data Encryption Standard (DES).

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

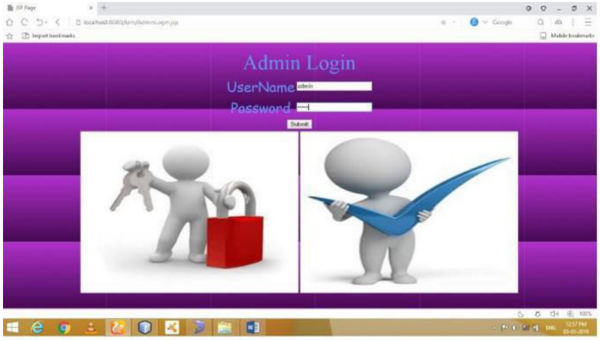
|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103072|

AES uses a block cipher, which means it encrypts data in fixed-sized blocks, typically 128 bits. It supports key sizes of 128, 192, or 256 bits, which determine the complexity of the encryption and the security level of the algorithm. AES is considered to be very secure and is widely used to encrypt sensitive data, such as financial transactions, medical records, and classified government communications. It is also used in many secure communication protocols, such as SSL/TLS, VPNs, and SSH. The algorithm works by applying a series of mathematical transformations, including substitution, permutation, and XOR operations, to the input data and the encryption key. The result is a ciphertext that appears random and unintelligible without the corresponding decryption key.

## V. RESULT

### ADMIN LOGIN

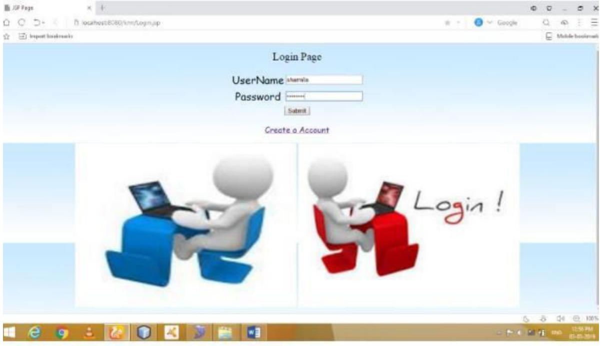


Admin Login

UserName admin

Password

### USER LOGIN

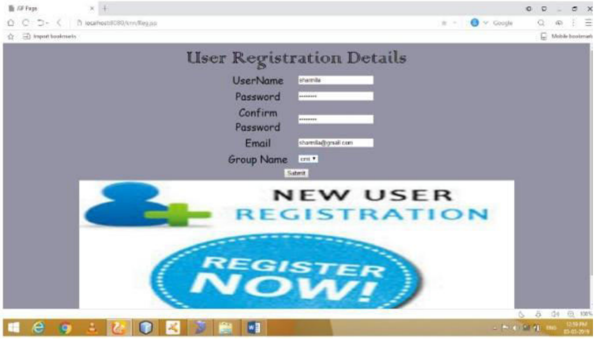


Login Page

UserName sharmila

Password

### USER REGISTRATION



User Registration Details

UserName sharmila

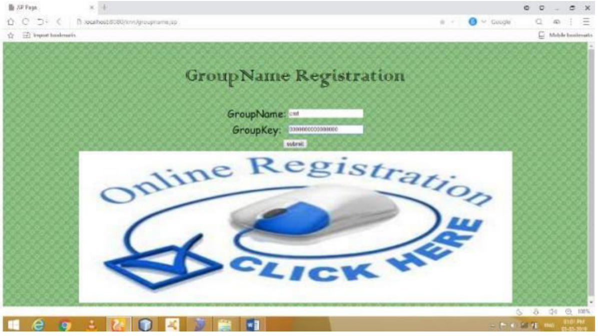
Password

Confirm Password

Email sharmila@gmail.com

Group Name cmt

### GROUP NAME REGISTRATION



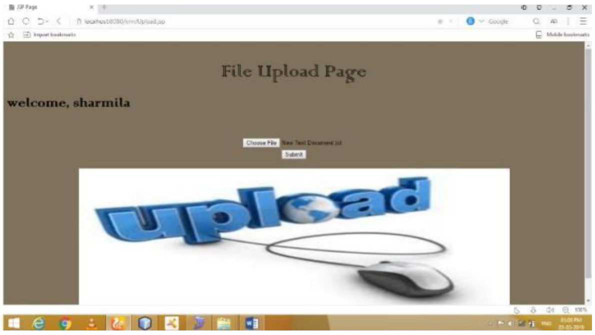
GroupName Registration

GroupName: cnt

GroupKey: 3999900000999000

submit

### UPLOAD PAGE



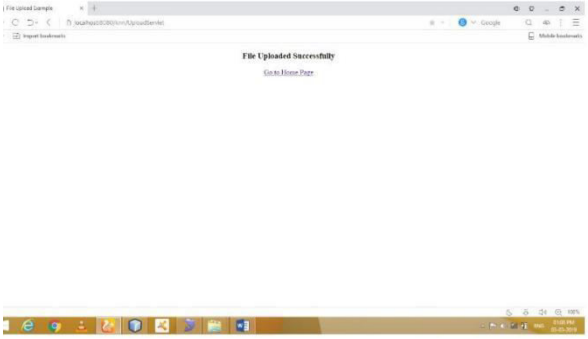
File Upload Page

welcome, sharmila

Choose File New Text Document.txt

Submit

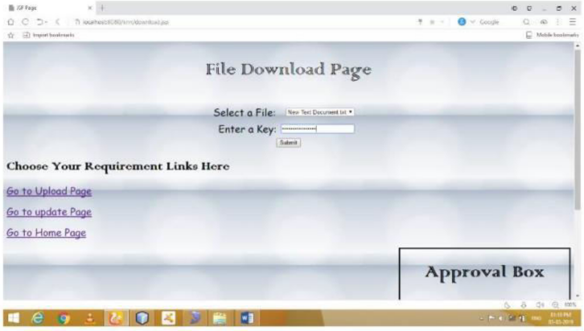
### UPLOAD PAGE



File Uploaded Successfully

Go to Home Page

### DOWNLOAD PAGE



File Download Page

Select a File: New Text Document.txt ▾

Enter a Key: ••••••••••••••••

Submit

Choose Your Requirement Links Here

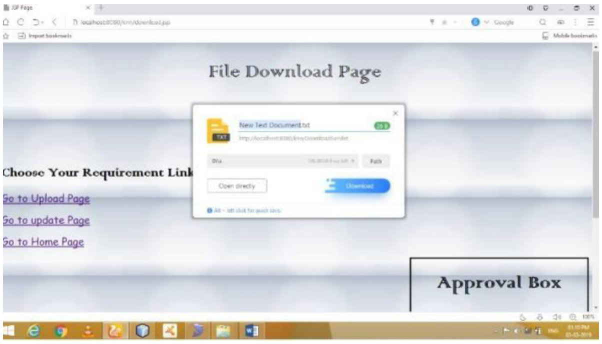
Go to Upload Page

Go to update Page

Go to Home Page

Approval Box

DOWNLOAD PAGE



File Download Page

Choose Your Requirement Link

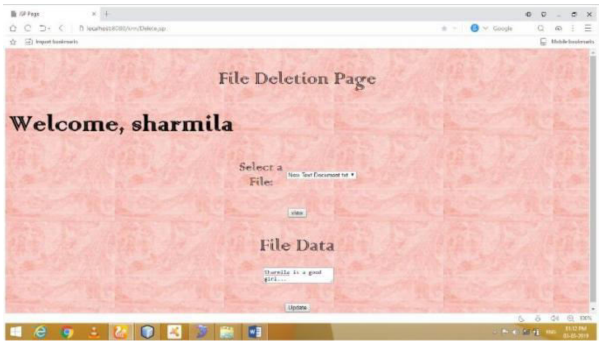
Go to Upload Page

Go to update Page

Go to Home Page

Approval Box

DELETION PAGE



File Deletion Page

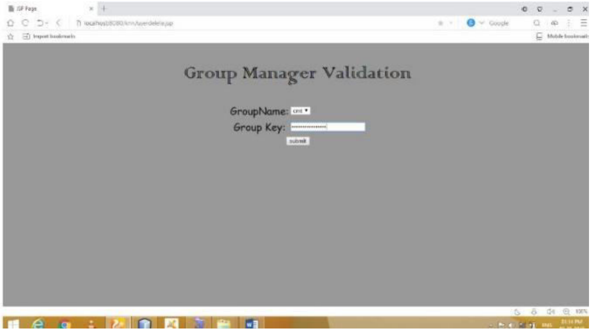
Welcome, sharmila

Select a File: New Text Document.txt

File Data

Sharmila is a good girl....

GROUP MANAGER VALIDATION

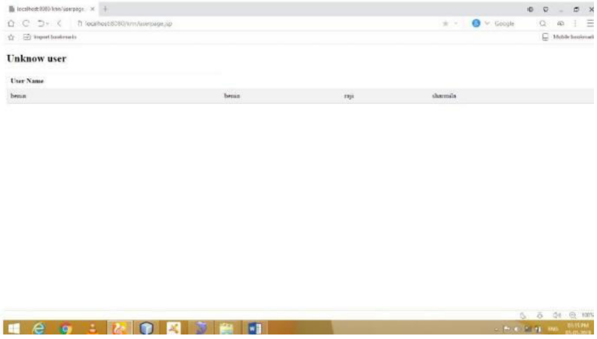


Group Manager Validation

GroupName: cni

Group Key: ••••••••••••

UNKNOWN USER



Unknow user

| User Name | | | |
|---|---|---|---|
| benan | benan | raja | sharmila |

### VI. CONCLUSION

Through the above summary, due to the problems about the collusion attacks that are widespread in the secure outsourcing of sequence comparison algorithms, this paper will introduce the trusted authority to authenticate user those who have the access to the data on cloud. SHA algorithm is used by the trusted authority to generate the key and that key will get share to user as well as the owner. The trusted authority module receives encrypted file using AES Algorithm from the data owner and computes hash value using MD-5 algorithm. It stores key in its database which will be used during the dynamic operations and to determine the cheating party in the system. Trusted authority send file to CSP module to store on cloud. The resulting key sets are shown to have a number of desirable properties that ensure the confidentiality of communication sessions against collusion attacks by other network nodes.

## REFERENCES

[1] A. K. Singh and I. Gupta, ‘‘Online information leaker identification scheme for secure data sharing,’’ Multimedia Tools Appl., vol. 79, no. 41,pp. 31165–31182, Nov. 2020.

[2] E. Zaghloul, K. Zhou, and J. Ren, ‘‘P-MOD: Secure privilege-based multilevel organizational data-sharing in cloud computing,’’ IEEE Trans. Big Data, vol. 6, no. 4, pp. 804–815, Dec. 2020.

[3] I. Gupta and A. K. Singh, ‘‘GUIM-SMD: Guilty user identification model using summation matrix-based distribution,’’ IET Inf. Secure., vol. 14, no. 6,pp. 773–782, Nov. 2020.

[4] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, ‘‘Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage,’’ IEEE Trans. Inf. Forensics Security, vol. 14, no. 2, pp. 331–346, Feb. 2019.

[5] I. Gupta and A. K. Singh, ‘‘An integrated approach for data leaker detection in cloud environment,’’ J. Inf. Sci. Eng., vol. 36, no. 5, pp. 993–1005,Sep. 2020.

[6] R. Li, C. Shen, H. He, X. Gu, Z. Xu, and C.-Z. Xu, ‘‘A lightweight secure data sharing scheme for mobile cloud computing,’’ IEEE Trans. Cloud Computing., vol. 6, no. 2, pp. 344–357, Apr. 2018.

[7] I. Gupta, N. Singh, and A. K. Singh, ‘‘Layer-based privacy and security architecture for cloud data sharing,’’ J. Common. Software. Syst., vol. 15, no. 2,pp. 173–185, Apr. 2019.

[8] J. Li, S. Wang, Y. Li, H. Wang, H. Wang, H. Wang, J. Chen, and Z. You, ‘‘An efficient attribute-based encryption scheme with policy update and file update in cloud computing,’’ IEEE Trans. Ind. Informat., vol. 15, no. 12,pp. 6500–6509, Dec. 2019.

[9] C. Suisse. (2017). 2018 Data Center Market Drivers: Enablers Boosting Enterprise Cloud Growth. Accessed: May 19, 2019. [Online]. Available: https://cloudscene.com/news/2017/12/2018-data-center-predictions/

[10] I. Gupta and A. K. Singh, ‘‘A framework for malicious agent detection in cloud computing environment,’’ Int. J. Adv. Sci. Technol., vol. 135, pp. 49–62, Feb. 2020.

# 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