# Enhancing Information Leakage in Multi Cloud Storage Facilities

**R. Sateesh[1], S. Haritha[2], S.N. Gowthami[3], C.MD. Farooq[4], S. Giridhar[5]**

*[1,2,3,4]UG Student, Department of Computer Science &Engineering, Mother Theresa Institute of Engineering & Technology, Palamaner, Andhra Pradesh, India.*

*[5]Assistant Professor of Computer Science & Engineering, Mother Theresa Institute of Engineering & Technology, Palamaner, Andhra Pradesh, India.*

----------***----------

**Abstract** - *In the present technology many schemes have been recently advanced for storing data in multiple clouds. Cloud Storage Providers (CSPs) provide storage for storing the data. The CSPs automatically leaks with a certain degree of user's information but there is no single point of attack can leak all the information. Hence the unplanned distribution of data chunks can lead to the high information disclosure even while using of the multiple clouds. Information leakage problem caused by unplanned data distribution in multicloud storage services. Then we introduce the StoreSim, an information leakage aware storage system in multicloud.*

***Key Words*: *Data chunk, Information leakage, MinHash, Multi cloud Storage, StoreSim.***

## 1.INTRODUCTION

Now-a-days with the increasingly rapid uptake of devices such as laptops, cell phones and tablets, users require a ubiquitous and massive network storage to handle their ever-growing digital lives. To meet these demands, many cloud-based storage and file sharing services such as Dropbox, Google Drive and Amazon S3, have gained popularity due to the easy-to-use interface and low storage cost. However, these centralized cloud storage services are criticized for grabbing the control of users' data, which allows storage providers to run analytics for marketing and advertising. Also, the information in users' data can be leaked e.g., by means of malicious insiders, backdoors, bribe and coercion. One possible solution to reduce the risk of information leakage is to employ multicloud storage systems in which no single point of attack can leak all the information. A malicious entity, such as the one revealed in recent attacks on privacy, would be required to coerce all the different CSPs on which a user might place her data, in order to get a complete picture of her data. File for each update to local, only parts with changed hash is uploaded. This synchronization is different from two different comparisons based on hash Line up and find the same file line by line.

## 2.EXSISTING SYSTEM

Now-a-days we store the data in multiple clouds. Distributing data over different cloud storage providers (CSPs) automatically provides users with a certain degree of information leakage. In existing system, we store the data in multiple clouds, if someone knows the data in single cloud then automatically guess the remaining data and we don't know whether the cloud provider is good bad. So, we don't give any guarantee to our data which are stored in multiple clouds. However, unplanned distribution of data chunks can lead to high information disclosure even while using multiple clouds.

### 2.1 DISADVANTAGES OF EXISTING SYSTEM:

1. No security for our data.
2. We don't know whether CSP good or bad.
3. There is a possibility to leak the information.

## 3.PROPOSED SYSTEM

To optimize the information leakage, we presented the StoreSim, an information leakage aware storage system in the multi cloud. StoreSim aims to store syntactically similar data on the same cloud, thus minimizing the user's information leakage across multiple clouds. StoreSim achieves this goal by using novel algorithm, MinHash which place the data with minimal information leakage (based on similarity) on the same cloud. We demonstrate that StoreSim is both effective and efficient (in terms of time and storage space) in minimizing information leakage during the process of synchronization in multi cloud.

### 3.1 ADVANTAGES OF PROPOSED SYSTEM:

1.Security for our data.
2.We can easily know whether CSP is good or bad.
3.There is no possibility to leak the information.

## 4. MODULES

**User:** Here user can first register after that user can login by using some credentials. After login user can view the profile and view the files and send the request to the CSP. And then view the response and then logout.

**CSP:** Here CSP can login by using username and password. And then cloud can view the users and upload the files by using file id and file name. Next cloud can view the file and view request to the user and then logout CSP.

**Admin:** First admin can login by using username and password. Next add the clouds and view the users and view the files and then logout.

## 5.RESULTS


**Fig -1: Admin Login**

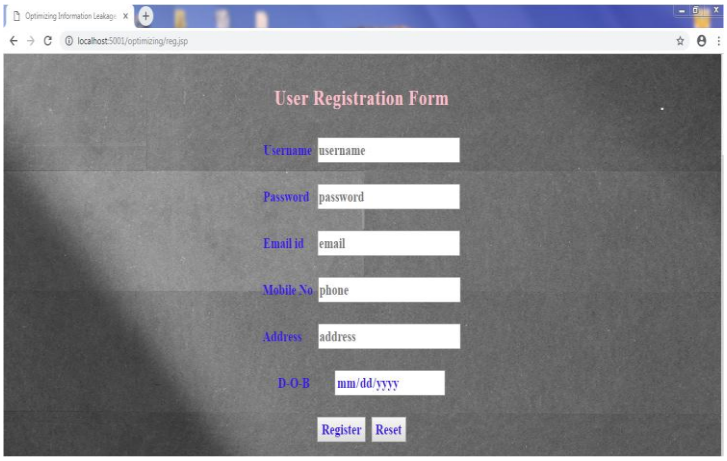


**Fig-2: User Registration**


**Fig -3: Add Clouds**

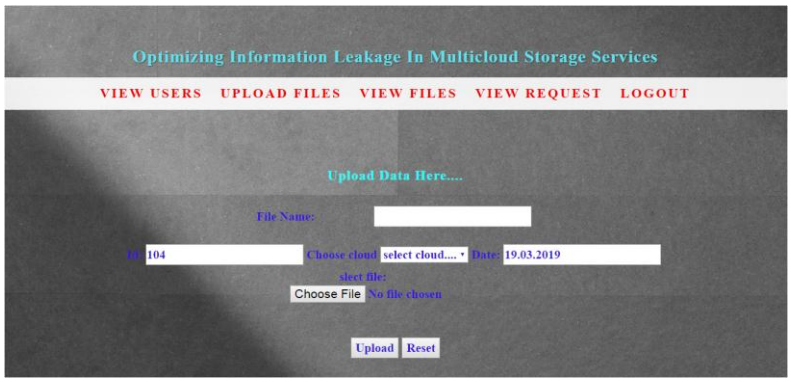


**Fig -4: Upload files**

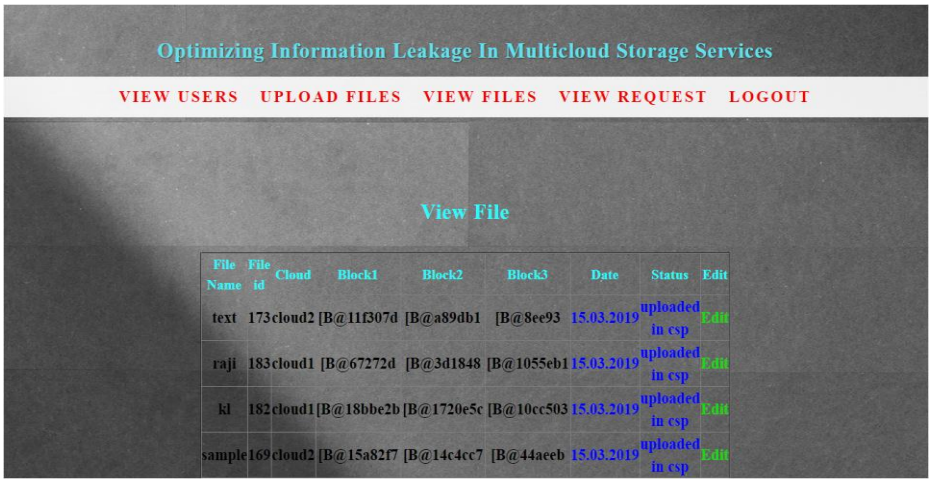


**Fig -5: View files**

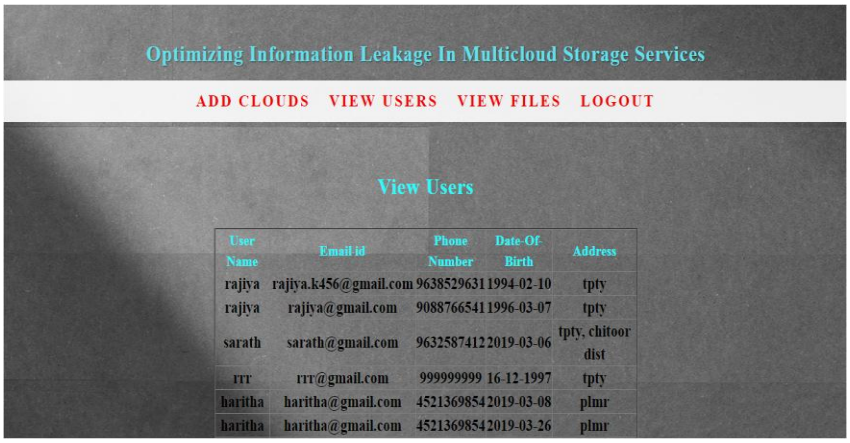


**Fig -6: View users**

## 5. CONCLUSIONS

Distributing data on multiple clouds provides users with a certain degree of information leakage control in that no single cloud provider is privy to all the user's data. However, unplanned distribution of data chunks can lead to avoidable information leakage. To optimize the information leakage, we presented the StoreSim, an information leakage aware storage system in the multicloud. StoreSim achieves this goal by using novel algorithm. MinHash, which place the data with minimal information leakage on the same cloud.

## 6. FUTURE ENHANCEMENT

- In our project, we show only whether the information is modified or not but not about where the information is modified and what information is modified.
- We get the notification through mail when information is modified.
- Include user password update option.

## REFERENCES

[1] Greenwald and E. MacAskill, "Nsa prism program taps in to user data of apple, google and others," The Guardian, 2013.

[2] Z. Wu, M. Butkiewicz, D. Perkins, E. Katz-Bassett, and H. V. Madhyastha, "Spanstore: Cost-effective geo-replicated storage spanning multiple cloud services," in Proceedings of the Twenty-Fourth ACM Symposium on Operating Systems Principles, pp. 292–308, ACM, 2013.

[3] P. Li and C. K¨onig, "b-bit minwise hashing," in Proceedings of the 19th international conference on World wide web, pp. 671–680, ACM, 2010.

## BIOGRAPHIES

**R. Sateesh**, R. Sateesh received M.Tech from JNTU ANANTAPUR. Presently working as Assistant professor in Computer Science and Engineering, **Mother Theresa Institute of Engineering & Technology. Palamaner, Andhra Pradesh, INDIA.**

**S. Haritha** S. Haritha doing her B.Tech degree in Computer Science & Engineering From **Mother Theresa Institute of Engineering & Technology, Palamaner, Andhra Pradesh, INDIA.**

**S.N. Gowthami** S.N. Gowthami doing her B.Tech degree in Computer Science & Engineering From **Mother Theresa Institute of Engineering & Technology, Palamaner, Andhra Pradesh, INDIA.**

**C.MD. Farooq** C.MD. Farooq doing his B.Tech degree in Computer Science & Engineering From **Mother Theresa Institute of Engineering & Technology, Palamaner, Andhra Pradesh, INDIA.**

**S. Giridhar** S. Giridhar doing his B.Tech degree in Computer Science & Engineering From **Mother Theresa Institute of Engineering & Technology, Palamaner, Andhra Pradesh, INDIA.**