Minimizing Data Leakage in Multi-Cloud Storage Service

R. Palson Kennedy [1], K. Varalakshmi[2]

[1,2] *Computer Science and Engineering, PERI Institute of Technology, Mannivakam, Chennai, India – 600048*

***Abstract* - In Provable Multi files Dynamic data Possession, Cloud Computing deals with stored data in Dynamic way to the cloud server. Multi-files Means, data to be copied in multiple servers. The project owner uploads the data in cloud server then automatically the data is multiple files then that files are stored in multiple servers. If the data is uploaded in multiserver the data loss is avoided from Hacking and server crash. In this project we introduced a new technique that is Fully Homomorphic Encryption (FHE) for taking Multi files of data, File security, Data Corrupted. In this Project we have a Fully Homomorphic Encryption algorithm to protect the data. That is keygen, copygen and tagged. Above process is done in Existing system using Single file of Dynamic Data.**

I.INTRODUCTION

This article proposes a symmetric key based cryptographic method named Proficient Security over Distributed Storage (PSDS) to secure client's information over the cloud. The client chooses whether the information is private (sensitive) or typical (normal) information. The information is split into two sections, part1 andpart2. After splitting the data, encryption steps of PSDS are applied to both parts. Both encrypted parts are uploaded to two separate clouds, cloud 1 and cloud 2 in order to prevent loss or exposure of data. Normal data is encrypted with PSDS encryption method and uploaded over a single cloud. The solid line shows encryption steps while the dotted line shows decryption steps. In the decryption phase, sensitive data. System architecture of the proposed PSDS. Clouds are downloaded and then merged in both parts. After merging, apply the decryption method of PSDS to convert cipher text into plain text. In the decryption process of normal data, the data is downloaded from a single cloud and then decryption is applied to transform cipher text to original text. PSDS is an adaptable approach as it is designed to achieve high security by splitting sensitive data on a multi-cloud mechanism. The proposed approach resists against different attacks such as Chosen Ciphertext attack, related key Attack and pollution attack. It also protects data against illegal access by the cloud service providers.

II.LITERATURE REVIEW AND PREVIOUSWORK

In previous System the data uploaded is stored in cloud server Single file way. Previously, data was stored in a single server and Owner shared the data with authorized users. Then authorized users send the file request to the file owner this is incorrect and service providers may access files illegally. So automatically data security loss occurs. In Existing, Somewhat Homomorphic Encryption (SHE) Algorithm was used.

1. Title: Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data.

Author: Ning Cao, Cong Wang, Ming Li, KuiRen, and Wenjing Lou Abstract: we define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing. We establish a set of strict privacy requirements for such a secure cloud data utilization system

2. Title: Verifiable Attribute-based Keyword Search over Outsourced Encrypted Data.

Author: QingjiZheng, ShouhuaiXu, and Giuseppe Ateniese. Abstract: It is common nowadays for data owners to outsource their data to the cloud. The solution allows a data user, whose credentials satisfy a data owner's access control policy, to (i) search over the data owner's outsourced encrypted data, (ii) outsource the tedious search operations to the cloud, and (iii) verify whether the cloud has faithfully executed the search operations.

3. Title: Multi-User Private Keyword Search for Cloud Computing

Author: Yanjiang Yang, Haibing Lu, and JianWeng. Abstract: Enterprises outsourcing their databases to the cloud and authorizing multiple users for access represents a typical use scenario of cloud storage services. In such a case of database outsourcing, data encryption is a good approach enabling the data owner to retain its control over the outsourced data. Searchable encryption is a cryptographic primitive allowing for private keyword-based search over the encrypted database

4. Title: A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data Author: Zhihua Xia, Xiongfei Wang, Xinghua Sun, and Qijie Wang **Abstract:** Due to the increasing popularity of cloud computing, more and more data owners are motivated to outsource their data to cloud servers for great convenience and reduced cost in data management. We construct a special tree-based index structure and propose a "Greedy Depth-first Search" algorithm to provide efficient multi-keyword ranked search. In order to resist statistical attacks, phantom terms are added to the index vector for blinding search results.

III. OUR SYSTEM'S ARCHITECTURE AND IMPLEMENTATION

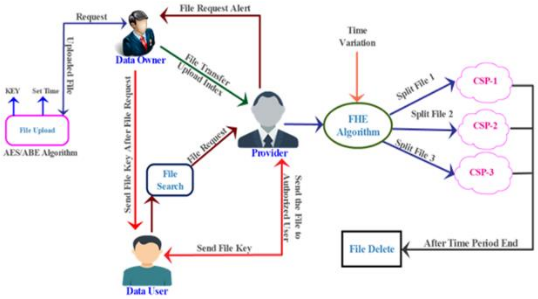


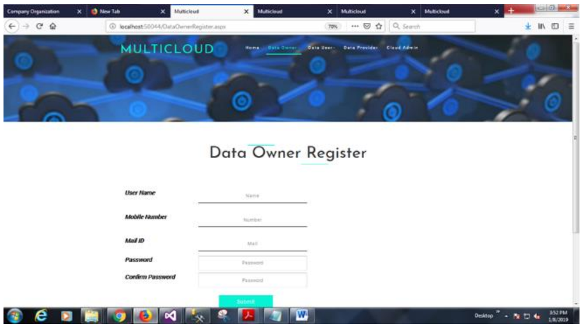
Figure 1. System Architecture

- In the implementation phase of this project, uploaded data is stored in multiple servers (Multi files). In proposed to one scheme FHE algorithms are used. If Owner uploads the data,

1. It automatically splits into three files then stored in three servers. To avoid server overload and for security. That copies the encrypted data. So Cloud Service Providers or any others can't hack the data.
2. Server automatically converts the file to zip formats. So the server reduces the file size automatically.

- Owner shares the file to the authorized user. Then the authorized users send the file request to the cloud server, then the server sends the encrypted data to the authorized user. And the authorized user gets the decrypt key from the data owner.

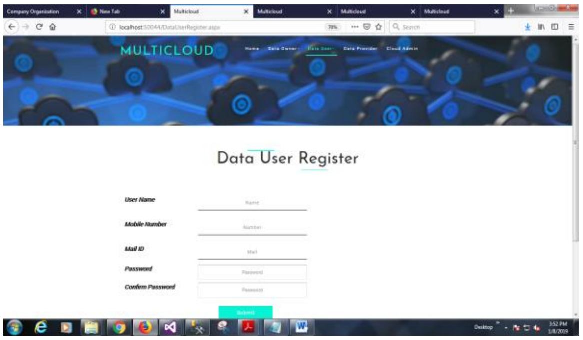
IV. OUTPUT SCREENSHOTS



Data Owner Register

User Name — Name
Mobile Number — Number
Mail ID — Mail
Password — Password
Confirm Password — Password

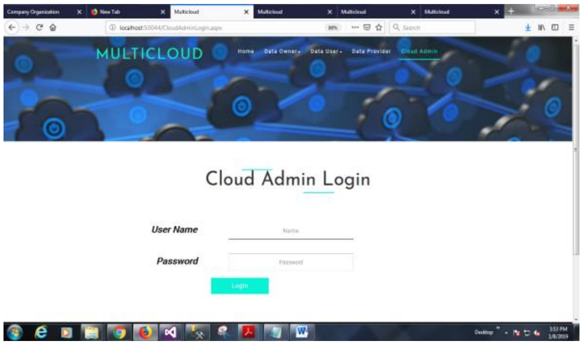
Figure 2. Owner Register



Data User Register

User Name — Name
Mobile Number — Number
Mail ID — Mail
Password — Password
Confirm Password — Password

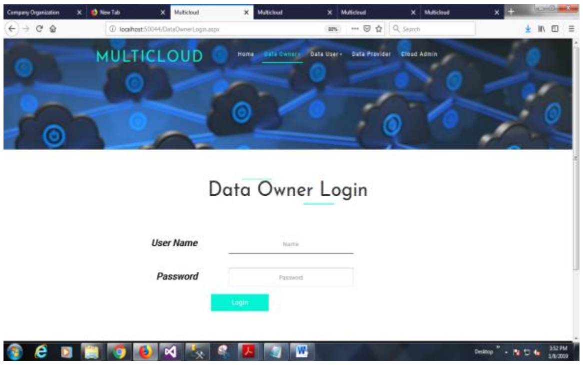
Figure 3. User Register



Cloud Admin Login

User Name — Name
Password — Password

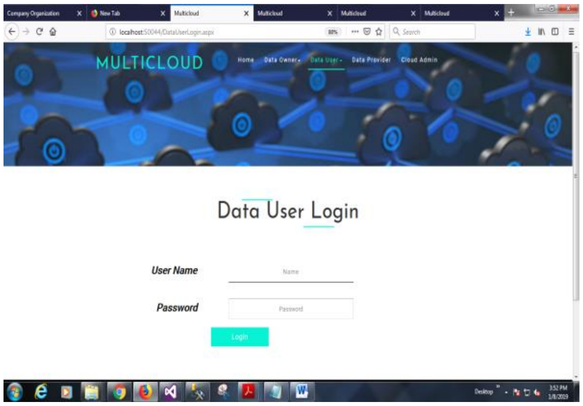
Figure 4. Cloud Admin Login



Data Owner Login

User Name — Name
Password — Password

Figure 5. Owner Login

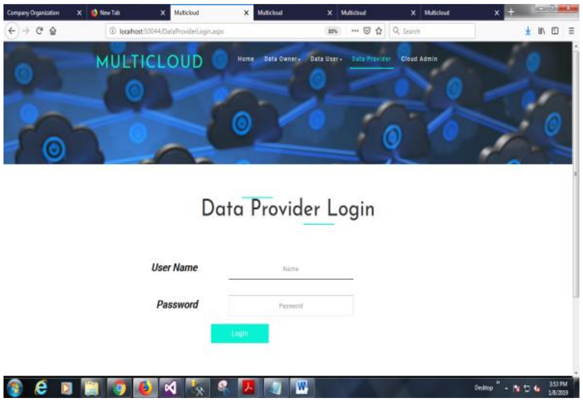


Data User Login

User Name: Name

Password: Password

Figure 6. User Login

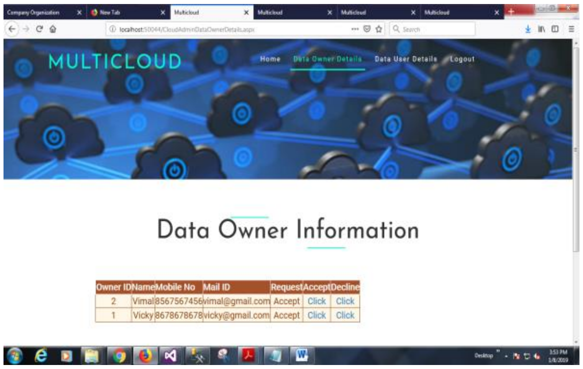


Data Provider Login

User Name: Name

Password: Password

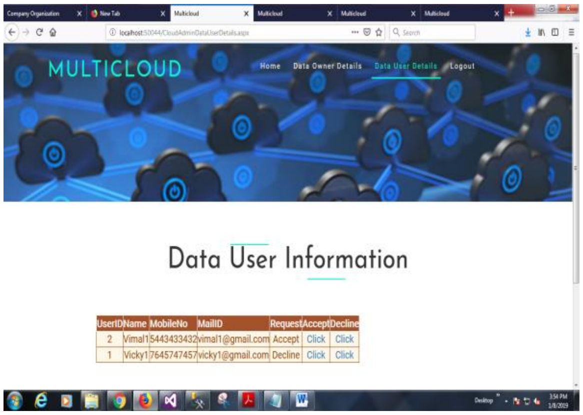
Figure 7. Service Provider Login



Data Owner Information

Owner ID	Name	Mobile No	Mail ID	Request	Accept	Decline
2	Vimal	8567567456	vimal@gmail.com	Accept	Click	Click
1	Vicky	8678678678	vicky@gmail.com	Accept	Click	Click

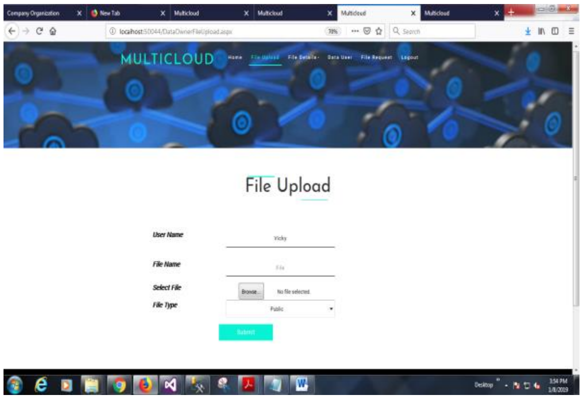
Figure 8. Data Owner Information



Data User Information

UserID	Name	MobileNo	MailID	Request	Accept	Decline
2	Vimal1	5443433432	vimal1@gmail.com	Accept	Click	Click
1	Vicky1	7645747457	vicky1@gmail.com	Decline	Click	Click

Figure 9. Data User Information



File Upload

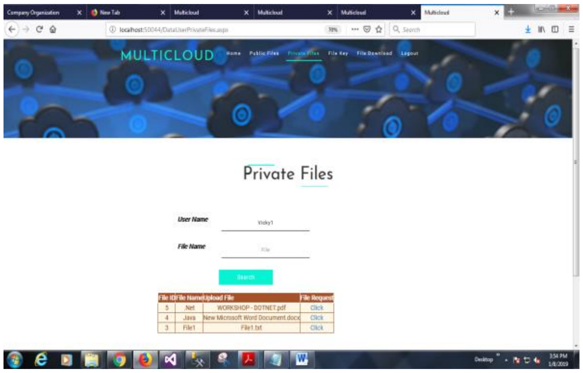
User Name: Vicky

File Name: File

Select File: No file selected.

File Type: Public

Figure 10. File Upload



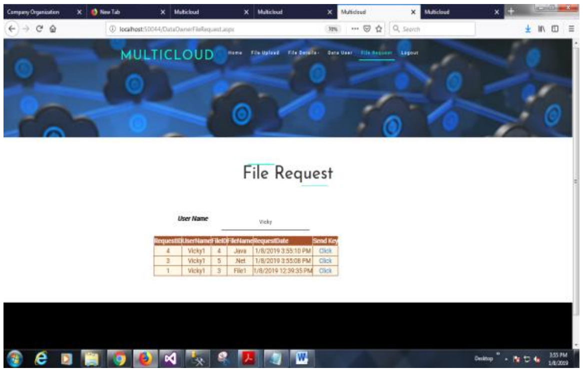
Private Files

User Name: Vicky1

File Name: File

File ID	File Name	Upload File	File Request
5	.Net	WORKSHOP - DOTNET.pdf	Click
4	Java	New Microsoft Word Document.docx	Click
3	File1	File1.txt	Click

Figure 11. File Details

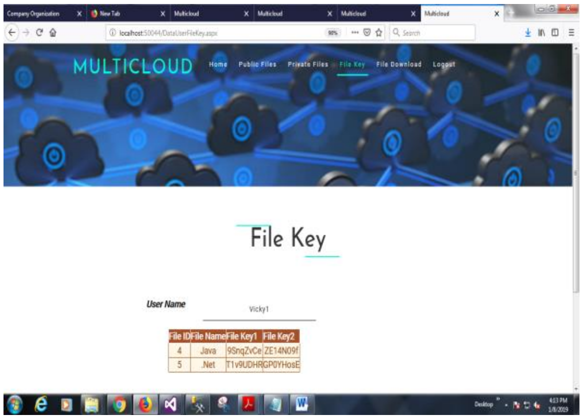


File Request

User Name: Vicky

RequestID	UserName	FileID	FileName	RequestDate	Send Key
4	Vicky1	4	Java	1/8/2019 3:55:10 PM	Click
3	Vicky1	5	.Net	1/8/2019 3:55:08 PM	Click
1	Vicky1	3	File1	1/8/2019 12:39:35 PM	Click

Figure 12. File Request

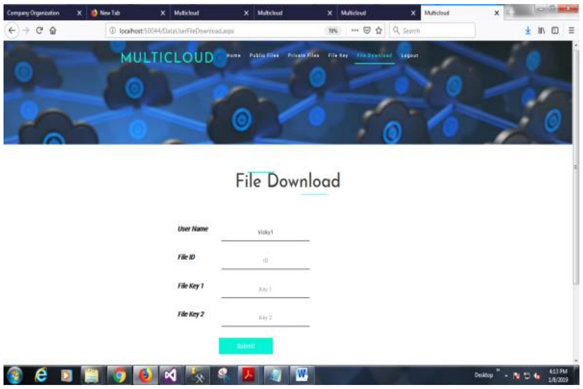


File Key

User Name: Vicky1

File ID	File Name	File Key1	File Key2
4	Java	9SnqZvCe	ZE14N09f
5	.Net	T1v9UDHR	GP0YHosE

Figure 13. File Key



File Download

User Name: Vicky1

File ID: ID

File Key 1: Key 1

File Key 2: Key 2

Figure 14. File Download

V.CONCLUSION

We proposed a hybrid scheme that combines public key encryption and fully homomorphic encryption. The proposed scheme is suitable for cloud computing environments since it has low storage requirements and supports efficient computing on encrypted data. Our solution provides the size of the transmitted Ciphertext and the conversion. The parameters of our hybrid scheme are very large when the message space of the FHE.

REFERENCES

[1] R. Barbulescu, P. Gaudry, A. Joux, and E. Thom´e. A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. IACR Cryptology ePrint Archive, 2014.

[2] J. Cheon, J.-S. Coron, J. Kim, M. Lee, T. Lepoint, M. Tibouchi, and A. Yun. Batch fully homomorphic encryption over the integers. In T. Johansson and P. Nguyen, editors, Advances in Cryptology - EUROCRYPT 2013, volume 7881 of Lecture Notes in Computer Science, pages 315–335. Springer Berlin Heidelberg, 2013.

[3] A. Joux. A new index calculus algorithm with complexity L(1/4+o(1)) in very small characteristics. IACR Cryptology ePrint Archive, 2014.

[4] S. Goldwasser and S. Micali. Probabilistic encryption. J. Comput. Syst. Sci., 28(2):270–299, 2015.

[5] J. Fan and F. Vercauteren. Somewhat practical fully homomorphic encryption. IACR Cryptology ePrint Archive, 2012:144, 2015.

[6] W. Li, K. Xue, Y. Xue and J. Hong, “TMACS: a robust and verifiable threshold multi-authority access control system in public cloud storage,” IEEE Trans. Parallel and Distributed Systems, vol. 27, no. 5, pp. 1484-1496, 2015

[7] J. Li, H. Wang, Y. Zhang and J. Shen, “Ciphertext-policy at-tribute-based encryption with hidden access policy and testing” KSII Transactions on Internet and Information Systems, vol. 10, no. 7, pp. 3339-3352, 2016.

[8] Z. J. Fu, K. Ren, J. G. Shu, X. M. Sun, and F. X. Huang, “Enabling personalized search over encrypted outsourced data with efficiency improvement,” IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 9, pp. 2546–2559, 2016.