

Improving Data Spillage in Cloud Storage Services

Mr.A.Anbumani¹, S.Surendar², V.K.Kabilan³, A.D.Akash Kumar⁴

Assistant Professor , Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India¹

U.G Students, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India^{2,3,4}

ABSTRACT: In this paper, Multiple files dynamic data possession in cloud computing deals with stored data in dynamic way to cloud service provider. Multiple files means, data to be copied in multiple server. In this project, owner to upload the data in cloud server automatically data to take multiple files then that files are stored in multiple server. To avoid the data loss from hacking and server crash upload the data in multiple servers. In this project we introduced new technique that is Fully Homomorphic Encryption(FHE) to take multiple files of data, file security, data corrupted. In this project we have FHE algorithm to protect the data. Above process in existing system is done using single file of dynamic data.

KEYWORDS: FHE(Fully Homomorphic Encryption), AES(Advanced Encryption Standard) , Data Leakage, Distributed Databases, Cloud service.

I. INTRODUCTION

In cloud computing world, the rapid increase of devices such as laptops, cellphones and tablets, users require an ubiquitous and massive network storage to handle their ever-growing digital lives. To require demands many files sharing systems and cloud-based storage such as Amazon S3, google drive, and dropbox, are the popular cloud based storage services. Due to its popularity, easy-to-use interface and low storage cost. This centralized cloud storage services are criticized for grabbing the control of users data, it allows cloud storage providers to run analytics for marketing and advertising. The users information such as data, audio, and video can be leaked. For example 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. we have the opportunity to minimize the total information that is leaked to each CSP(Cloud Service Provider)[1]. Therefore, we need more sophisticated techniques to detect the nearduplicate(or similar) data chunks to reduce the information leakage in the multicloud storage system.

II. LITERATURE REVIEW

Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou

“Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data”,2014

The first time, we define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE). We establish a set of strict privacy requirements for such a secure cloud data utilization system. We further use “inner product similarity” to quantitatively evaluate such similarity measure. We first propose a basic idea

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Special Issue 2, March 2019

for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. To improve search experience of the data search service, we further extend these two schemes to support more search semantics. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given. Experiments on the real-world data set further show proposed schemes indeed introduce low overhead on computation and communication[2].

Qingji Zheng, Shouhuai Xu, and Giuseppe Ateniese

VABKS: “Verifiable Attribute-based Keyword Search over Outsourced Encrypted Data”,2014

It is common nowadays for data owners to outsource their data to the cloud. Since the cloud cannot be fully trusted, the outsourced data should be encrypted. This however brings a range of problems, such as: How should a data owner grant search capabilities to the data users? How can the authorized data users search over a data owner’s outsourced encrypted data? How can the data users be assured that the cloud faithfully executed the search operations on their behalf? Motivated by these questions, we propose a novel cryptographic solution, called verifiable attribute-based keyword search (VABKS). 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].

Yanjiang Yang, Haibing Lu, and Jian Weng.

“Multi-User Private Keyword Search for Cloud Computing”, 2011

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. The above setting of enterprise outsourcing database to the cloud requires multi-user searchable encryption, whereas virtually all of the existing schemes consider the single-user setting. To bridge this gap, we are motivated to propose a practical multi-user searchable encryption scheme, which has a number of advantages over the known approaches. The associated model and security requirements are also formulated. We further discuss to extend our scheme in several ways so as to achieve different search capabilities[4].

Zhihua Xia, Xiongfei Wang, Xinghua Sun, and Qijie Wang

“A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data”,2016

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. However, sensitive data should be encrypted before outsourcing for privacy requirements, which obsoletes data utilization like keyword-based document retrieval. In this paper, we present a secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations like deletion and insertion of documents. We construct a

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Special Issue 2, March 2019

special tree-based index structure and propose a “Greedy Depth-first Search” algorithm to provide efficient multi-keyword ranked search. The secure kNN algorithm is utilized to encrypt the index and query vectors, and meanwhile ensure accurate relevance score calculation between encrypted index and query vectors. In order to resist statistical attacks, phantom terms are added to the index vector for blinding search results[5].

Wenhai Sun, Shucheng Yu, Wenjing Lou, Y Thomas Hou, and Hui Li

“Protecting Your Right: Attribute-based Keyword Search with Fine-grained Owner-enforced Search Authorization in the Cloud”,2014

Search over encrypted data is a critically important enabling technique in cloud computing, where encryption-before outsourcing is a fundamental solution to protecting user data privacy in the untrusted cloud server environment. Many secure search schemes have been focusing on the single-contributor scenario, where the outsourced dataset or the secure searchable index of the dataset are encrypted and managed by a single owner, typically based on symmetric cryptography. In this paper, we focus on a different yet more challenging scenario where the outsourced dataset can be contributed from multiple owners and are searchable by multiple users, i.e. multi-user multi contributor case. Inspired by attribute-based encryption

(ABE), we present the first attribute-based keyword search scheme with efficient user revocation (ABKS-UR) that enables scalable fine-grained (i.e. file-level) search authorization. Our scheme allows multiple owners to encrypt and outsource their data to the cloud server independently. Users can generate their own search capabilities without relying on an always online trusted authority. Fine-grained search authorization is also implemented by the owner-enforced access policy on the index of each file[6].

III. PROPOSED SYSTEM

In proposed system data's are stored in multiple server (Multi files) using FHE algorithm.If owner upload the data, automatically prepare three files then stored in three server for security and to avoid server overload. That files also encrypted so cloud service provider or cant be hacked. If owner upload the data, server automatically convert to zip format. So server reduce the file size automatically. Owner share the file to authorized user. Then authorized user send the file request to cloud server again server send the encrypted data to authorized user. And authorized user get the decrypt key from data owner.

International Journal of Innovative Research in Science, Engineering and Technology

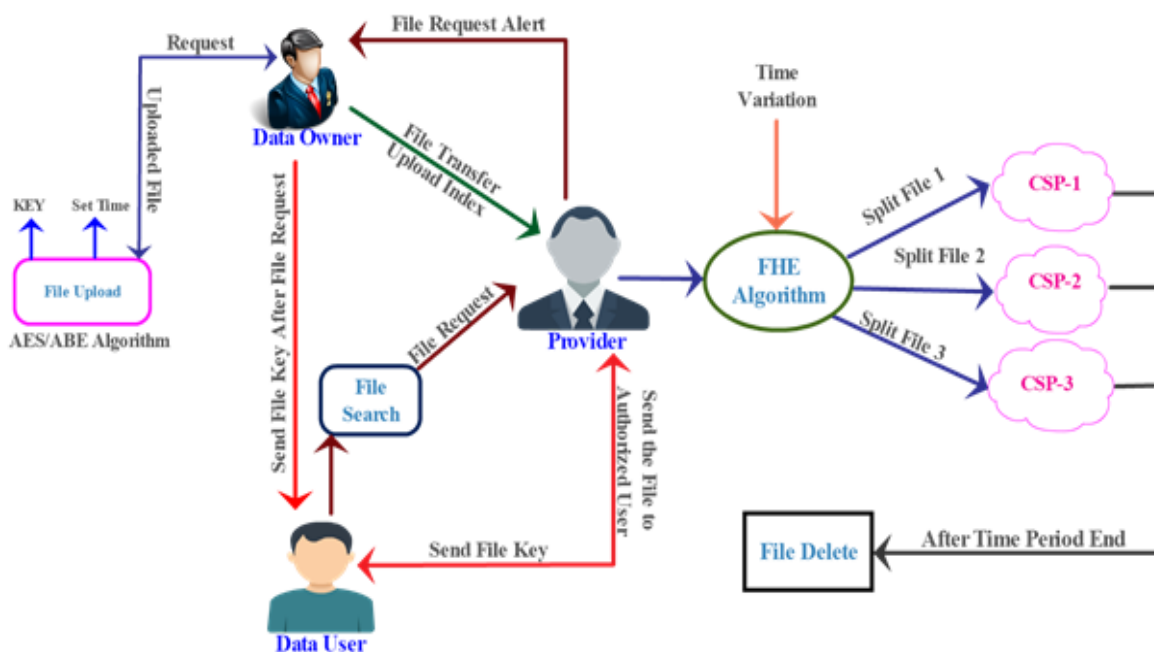
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

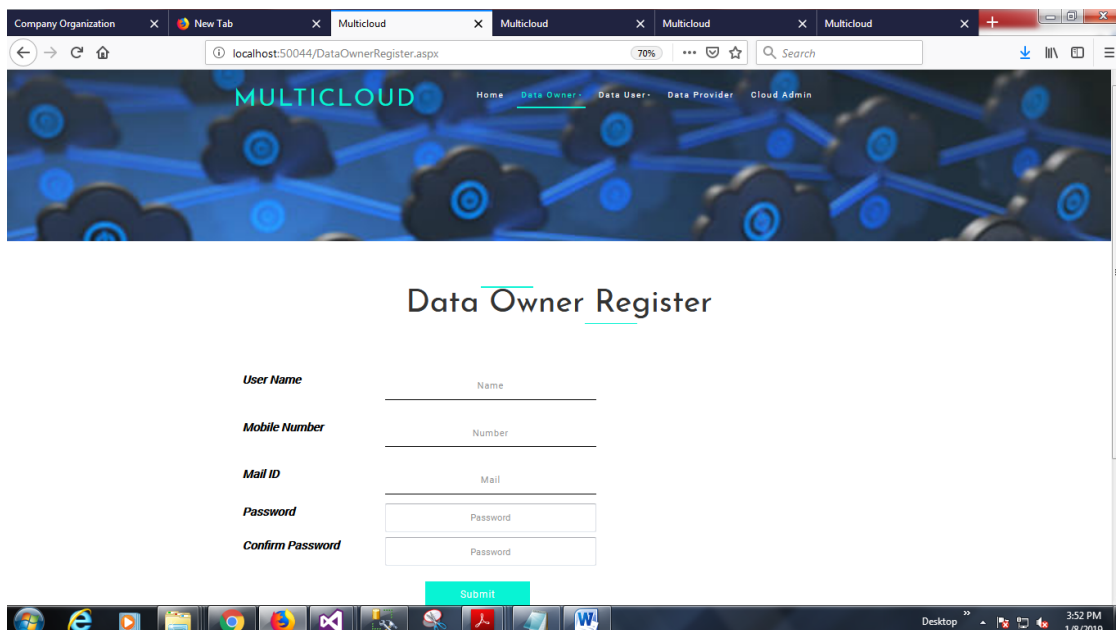
Vol. 8, Special Issue 2, March 2019

IV. PROPOSED SYSTEM

ARCHITECTURE DIAGRAM



Owner Register



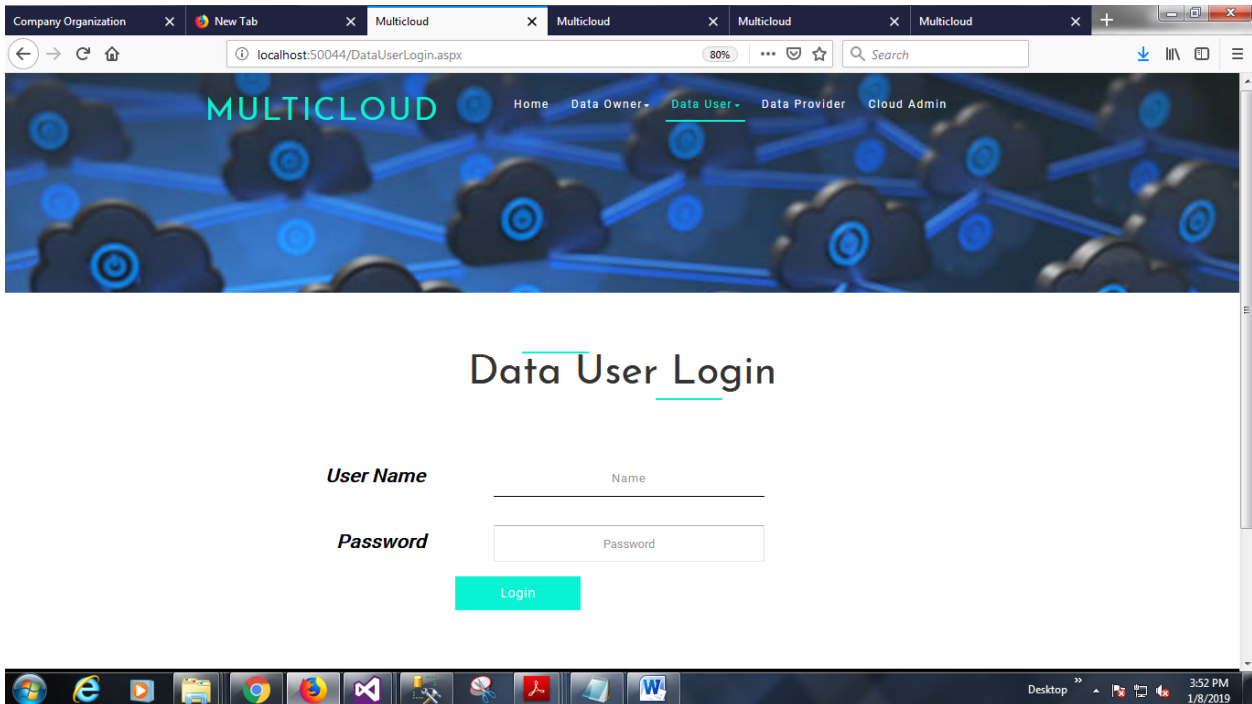
International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

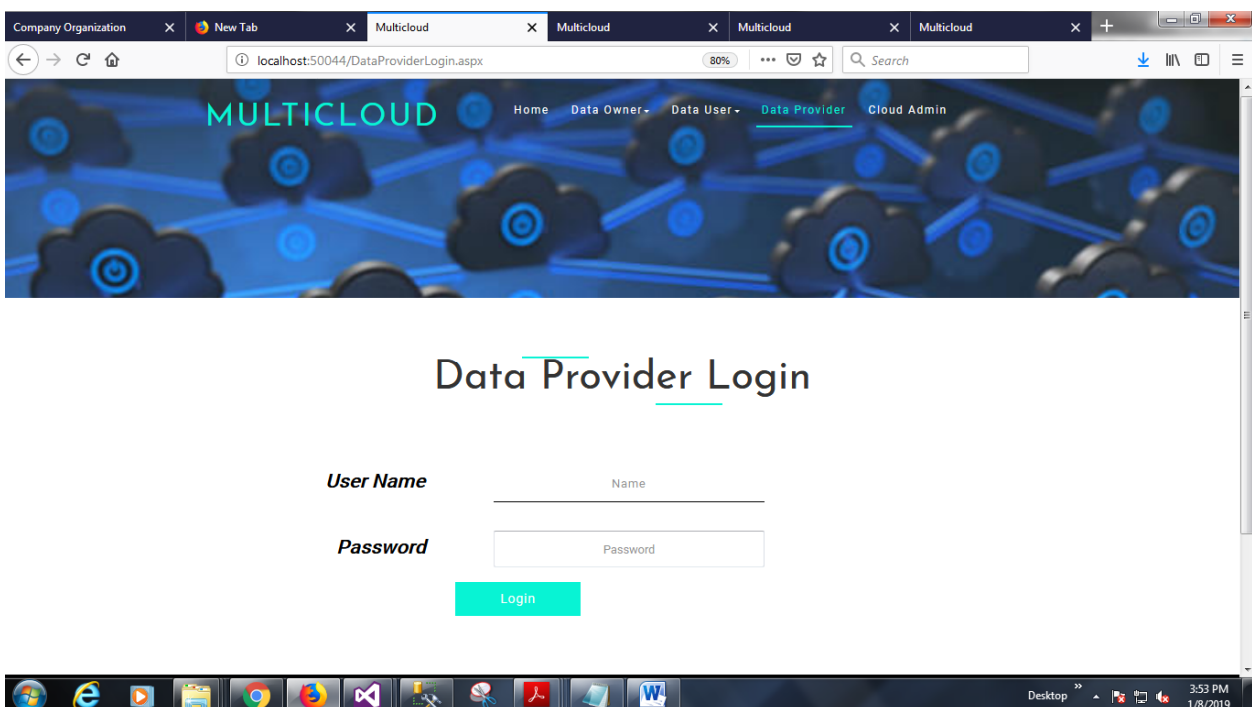
Vol. 8, Special Issue 2, March 2019

User Login



The screenshot shows a web browser window with the URL localhost:50044/DataUserLogin.aspx. The page features a header with the 'MULTICLOUD' logo and navigation links: Home, Data Owner, Data User (selected), Data Provider, and Cloud Admin. The main content area is titled 'Data User Login' and contains a form with two input fields: 'User Name' (with a placeholder 'Name') and 'Password' (with a placeholder 'Password'). A green 'Login' button is positioned below the fields. The Windows taskbar at the bottom shows the system clock as 3:52 PM on 1/8/2019.

Provider Login



The screenshot shows a web browser window with the URL localhost:50044/DataProviderLogin.aspx. The page features a header with the 'MULTICLOUD' logo and navigation links: Home, Data Owner, Data User, Data Provider (selected), and Cloud Admin. The main content area is titled 'Data Provider Login' and contains a form with two input fields: 'User Name' (with a placeholder 'Name') and 'Password' (with a placeholder 'Password'). A green 'Login' button is positioned below the fields. The Windows taskbar at the bottom shows the system clock as 3:53 PM on 1/8/2019.

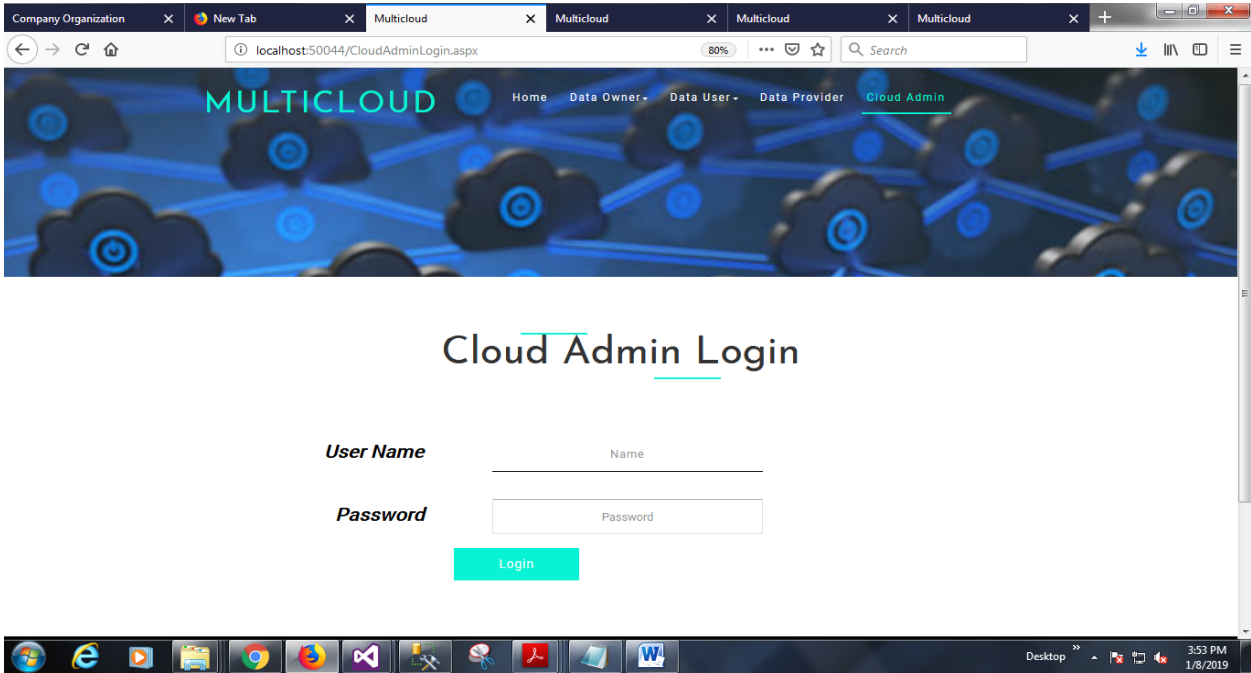
International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

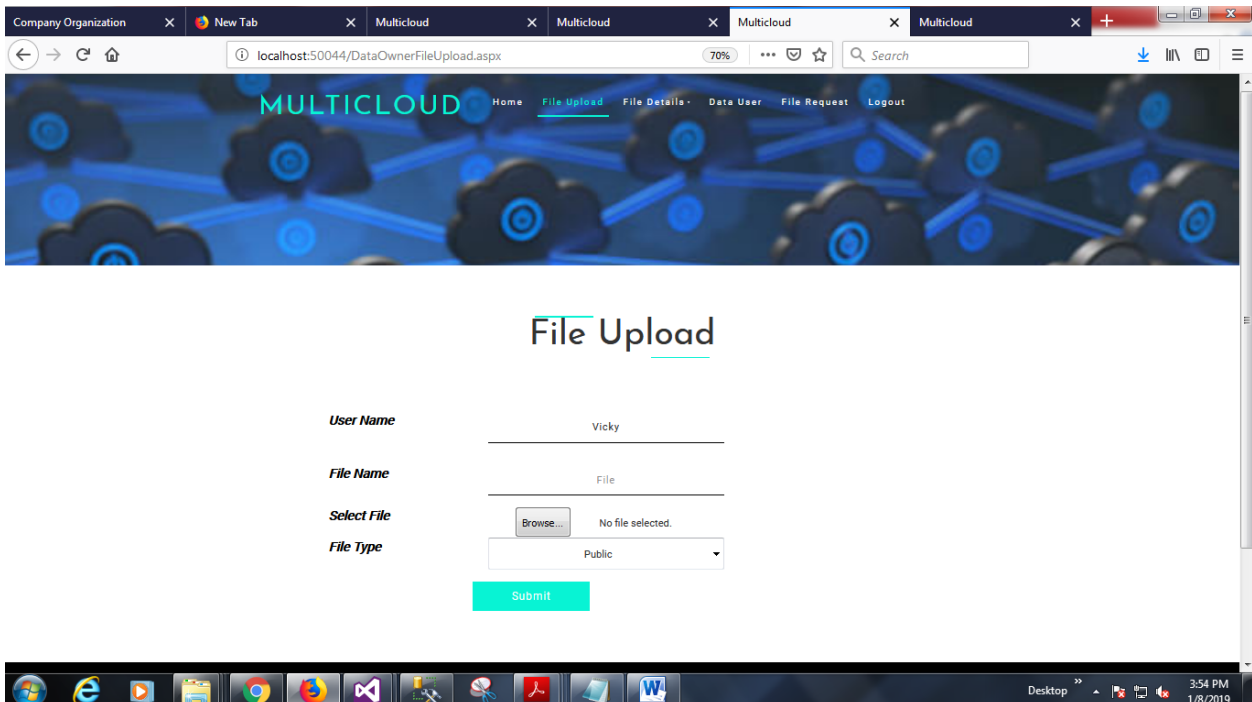
Visit: www.ijirset.com

Vol. 8, Special Issue 2, March 2019

Cloud Admin Login



File Upload



International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

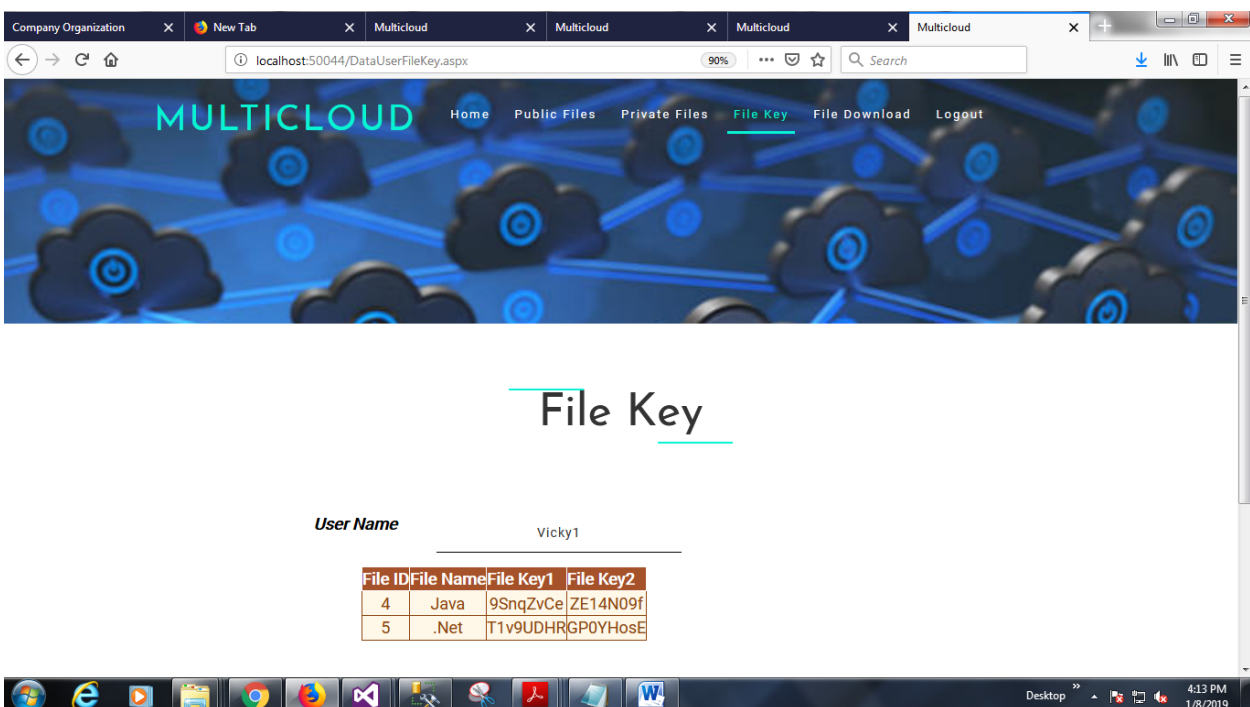
Vol. 8, Special Issue 2, March 2019

File Request



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

File Key



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

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

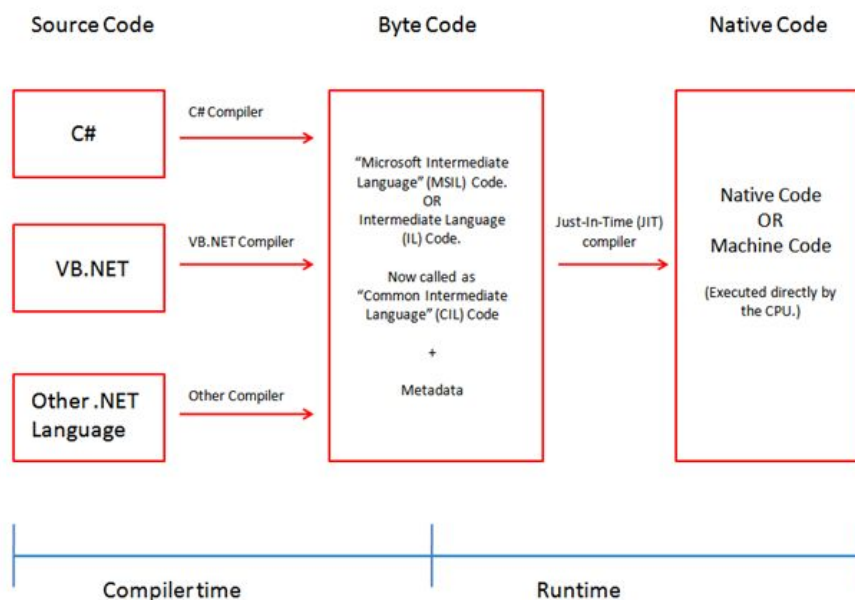
Visit: www.ijirset.com

Vol. 8, Special Issue 2, March 2019

V. TECHNOLOGIES USED

.Net:

Microsoft .NET technology you will have access to a new generation of advanced software joining the best of computing and communications in a revolutionary new way. The effect will be to totally transform the Web and every other aspect of the computing experience. .NET enables developers, businesses, and consumers to harness technology on their terms.



VI. CONCLUSION

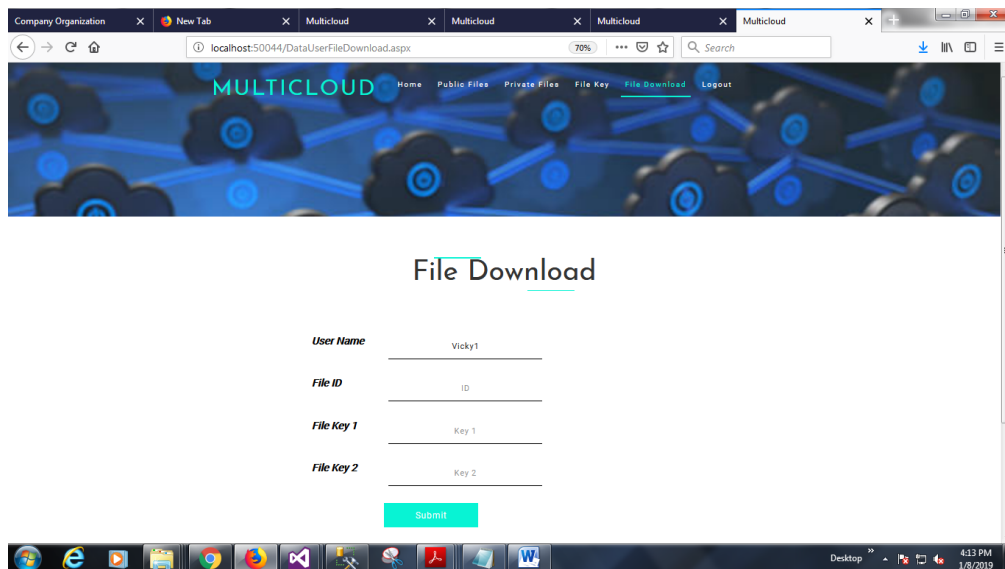
- We proposed a hybrid scheme that combines public key encryption and fully homomorphic encryption.
- The proposed scheme is suitable for cloud computing environments since it has low storage requirement, and supports efficient computing on encrypted data.
- Our solution provides the size of the transmitted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

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Special Issue 2, March 2019



Future Enhancement:

In this have to add extra features in future like

1. Send Alert Notification details to send via send SMS.
2. In future in this concept to in android app.

REFERENCES

- [1] R. Barbulescu, P. Gaudry, A. Joux, and E. Thomé. 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 characteristic. 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 attribute-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.