

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES
ENHANCED KEY DISTRIBUTION FOR FILE SHARING USING FUZZY
AUTHORIZATION MODEL**P.Priyanka^{*1} & Dr.M.Jagadeesan²**^{*1}Pg Scholar - Department of Computer Applications, Kongu Engineering College, Perundurai,
Tamilnadu, India² Asst. Professor - Department of Computer Applications, Kongu Engineering College, Perundurai,
Tamilnadu, India**ABSTRACT**

A cloud system is difficult to synchronize login and authentication data between external clouds and internal systems without exposing internal security data. The cloud technologies are rapidly being adopted throughout the Information Technology (IT) due to their various attractive properties. In spite of their spread, they have raised a range of significant security and privacy concerns which interrupt their adoption in sensitive environments. The cloud computing technology provides IT services and resources to the customers through public network such as internet. The cloud computing services and infrastructure are mostly owned by a third party called cloud service providers. Cloud computing provides an innovative model for the organizations to use software applications, storage and processing capabilities of cloud without investing on the infrastructure. To ensure a correctness of users' data in the cloud, we propose an effective and secure distributed model including a Self-Proxy Server (SPS) with self-created algorithm a distributed SPS dynamically interacts with Key Manager (KM) when the mobile users take on cloud services.

Keywords: *login and authentication, cloud computing, Self-Proxy Server (SPS), Key Manager.*

I. INTRODUCTION

Mobile computing is human –computer interaction by which a computer is expected to be transported during normal usage, which allows for transmission of data, voice and video. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad hoc networks and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications Portability: Facilitates movement of device(s) within the mobile computing environment. Connectivity: Ability to continuously stay connected with minimal amount of lag/downtime, without being affected by movements of the connected node Social Interactivity: Maintaining the connectivity to collaborate with other users, at least within the same environment. Individuality: Adapting the technology to suit individual needs. Mobile Computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link. The mobile communication in this case, refers to the infrastructure put in place to ensure that seamless and reliable communication goes on. These would include devices such as protocols, services, bandwidth, and portals necessary to facilitate and support the stated services.

II. LITRATURE SURVEY**1. Analysis of the cloud computing security problem**

MOHAMED AL MORSY, JOHN GRUNDY AND INGO MÜLLER

Cloud computing provides the next generation of internet based, highly scalable distributed computing systems in which computational resources are offered 'as a service'.

Multi-tenancy and elasticity are two key characteristics of the cloud model. Elasticity enables scaling up and down resources allocated to a service based on the current service demands. Both characteristics focus on improving resource utilization, cost and service availability.

The cloud model has motivated industry and academia to adopt cloud computing to host a wide spectrum of applications ranging from high computationally intensive applications down to light weight services. The model is also well-suited for small and medium businesses because it helps adopting IT without upfront investments in infrastructure, software licenses and other relevant requirements

Google Apps and Microsoft Windows Azure are the most known - Software-as-a-service (SaaS) applications hosted on the cloud infrastructure as internet based service for end users, applications on the customers' computers.

2. The management of security cloud computing

Ramgovind S, Eloff MM, Smith E

Cloud computing has elevated IT to newer limits by offering the market environment data storage and capacity with flexible scalable computing processing power to match elastic demand and supply, whilst reducing capital expenditure.

The success of modern day technologies highly depends on its effectiveness of the world's norms, its ease of use by end users and most importantly its degree of information security and control.

3. Data security in unreliable cloud using access control and access time

Pooja A. Uplenchwar, L. H. Patil

A cloud is basically a large scale distributed system where a data owner's data is replicated over multiple servers for high availability. An alternative solution is to apply the proxy re-encryption (PRE) technique. This approach [13] takes advantage of the abundant resources in a cloud by delegating the cloud to re-encrypt data. This approach is also called command driven reencryption scheme, wherever cloud servers execute re encryption while receiving commands from the data owner. However, command-driven re-encryption schemes do not consider the underlying system architecture of the cloud environment. In this paper consider a cloud computing environment consisting of a data owner, a cloud service provider (CSP) and multiple data users.

4. Structured encryption and controlled disclosure

Melissa Chase and Seny Kamar

The model for structured encryption, the formal security definition and several efficient constructions. The present schemes for performing queries are two simple types of structured data, specifically lookup queries on matrix-structured data, and search queries on labeled data.

The most common use of encryption is to provide confidentiality by hiding all useful information about the plaintext. Encryption, however, often renders data useless in the sense that one loses the ability to operate on it. At a high level, a structured encryption scheme takes as input structured data (δ, m) and outputs an encrypted data structure γ and a sequence of cipher texts $c = (c_1, \dots, c_n)$. Using the private key, a token τ can be constructed for any query such that pointers to the encryptions of $(m_i)_{i \in I}$ can be recovered from γ and τ . Furthermore, given the private key, one can decrypt any cipher text c_i . A certain class of symmetric searchable encryption (SSE) schemes

III. PROPOSED SYSTEM METHODOLOGY

Administrator Module

In this module, the admin user can able to add the cloud service provider details, application provider details and data owner details, the details which are stored into the corresponding tables in the data base.

Cloud Service Provider details includes the Cloud service provider id, name of the cloud provider, website and password details will be stored into the CSPProviders table. Application Service Provider details includes the Application service provider id, name of the application service provider, password are stored into the ASProviders table. Data Owner details includes the data owner id, name of the data owner and password details are stored into the DataOwner table.

Also the admin user assigns the Cloud Service Provider to Application Service Provider and Assign Cloud Service Provider to Data Owner. And the admin user can able to view the Cloud Service Providers details, Application Service Providers details, Data Owners Details; View Users details and view downloads details.

The screenshot shows a web browser window with the URL `localhost:1495/DistributedMobileCloudComputingForBigData/default.aspx`. The main content area features a diagram titled "Public Key Encryption" illustrating the flow from a Sender to a Receiver. The process involves encryption using the Receiver's Public Key to create Cipher Text, which is then decrypted using the Receiver's Private Key. A note states "Both Keys Are Different". Below the diagram is a navigation menu with links: Home, Admin Login, CSP(Self-Proxy) Login, Data Owner Login, User Registration, and User Login. The text below the menu describes the mobile cloud computing technique, its security benefits, and the role of a Self-Proxy Server (SPS) in interacting with a Key Manager (KM).

Self Proxy Server (SPS) Module

A solution is to apply a distributed self proxy re encryption technique, propose a Self Proxy Server (SPS). It coordinates and chooses keys by Key Manager (KM) whenever group membership changes. The distributed SPS provides not only encryption and decryption keys but also immediate re encryption keys for shared data. After communicating with KM, it automatically receives necessary keys from KM by self created algorithm. A distributed SPS scheme is one solution where multiple proxies are automatically deployed in several clouds.

In this Module, the cloud service provider can able to login with their provided credentials and can able to View Application Service Provider Details, View Data Owner Details. In this module the Payment from Data Owner will be performed. The details includes of the payments are Cloud storage provider id, data owner id, date of payment, file details and the payment amount.

The screenshot displays a web browser window with a blue header and a navigation menu. The main content area features a diagram titled 'Public Key Encryption' showing a sender encrypting a 'TXT' file using a 'Recipient's Public Key' to create 'Cipher Text', which is then decrypted by a 'Receiver' using their 'Recipient's Private Key'. Below the diagram is a navigation bar with links: Home, Admin Login, CSP(Self-Proxy) Login, Data Owner Login, User Registration, and User Login. The main content area is titled 'ADD CLOUD STORAGE PROVIDER' and contains a form with the following fields: CSPProvider ID (105), CSPProvider Name (iWeb), E-Mail ID (info@iweb.com), Website (https://iweb.com), and Password (masked with dots). There are 'Add New' and 'Save' buttons, and a 'Delete' button with a dropdown menu. A message at the bottom of the form reads 'Cloud Storage Provider Details Saved'.

Data Owner Module

The Data Owner (DO) has data to be stored in the cloud and rely on the cloud for data computation, consists of both individual consumers and organizations. The data owner of MCP shares data to many other cloud users. The data is encrypted with a key from KM and then stored in the cloud along with access control list indicating the user group. Upon access request from a user, the cloud communicates with SPS, based on access control list, and Self Proxy Server (SPS) requests for the key.

According to the key request to the SPS, uses re-encryption to transfer the encrypted format that can be decrypted by the user’s private key. The user can download the encrypted data from the cloud and use the decryption key. In this data owner module, the data owner can View the Application service provider Details, View CSP Details after logged into the system.

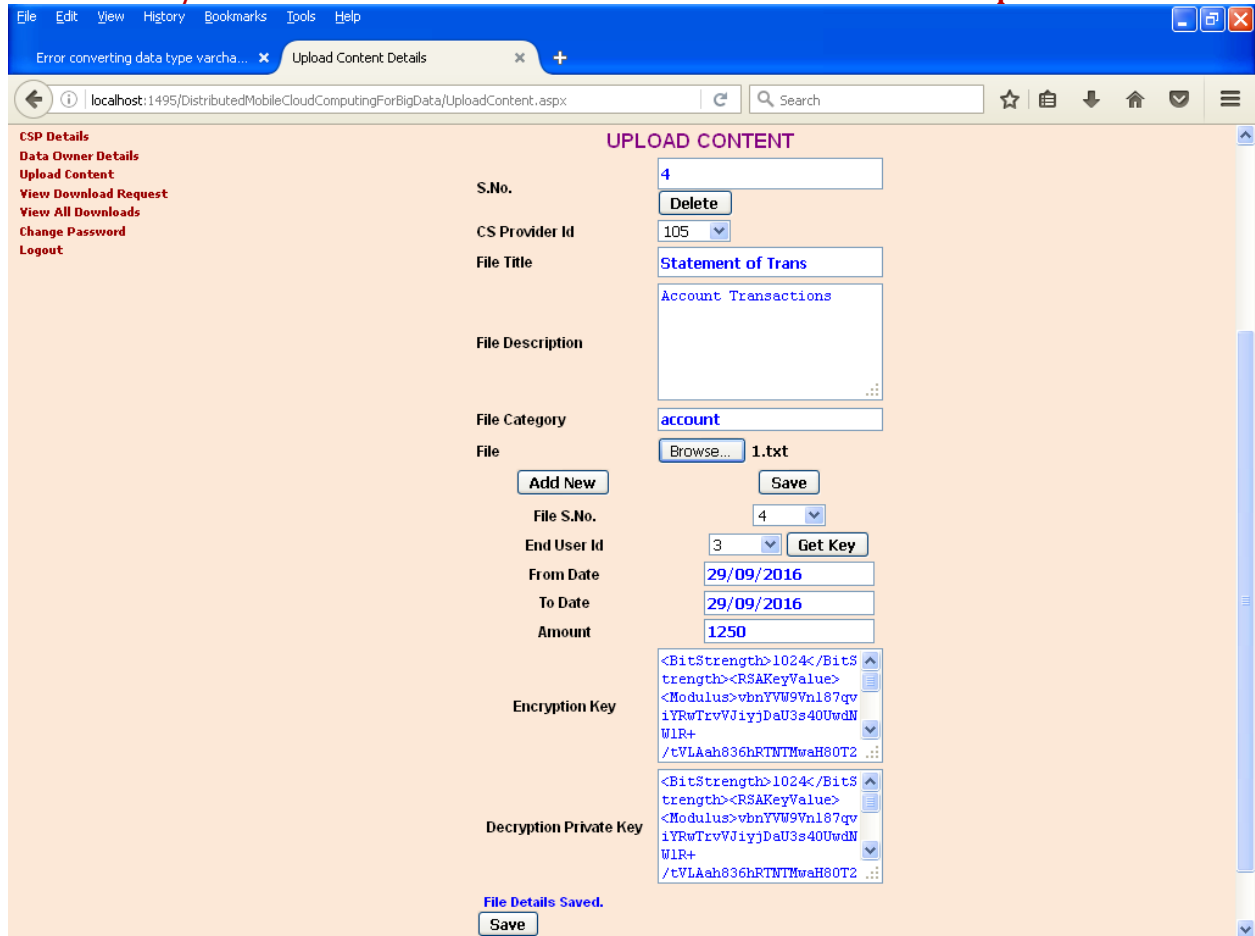
The data owner can also Upload Content to the cloud storage with the description of file description, category of the file and cloud storage provider details along with application service provider details. The data owner can also View the Download Request from the users and Provide Keys to the download request files by the end users.

DATA OWNERS LIST

DataOwnerId	DataOwnerName	EMailId	WebSite
1	State Bank of India	contact@sbi.com	http://www.sbi.com
2	HDFC Bank	contact@hdfc.com	http://www.hdfc.com
3	HSBC Bank	contact@hsbc.com	http://www.hsbc.com
4	Karur Vysya Bank	contact@kvb.com	http://www.kvb.com
5	Dena Bank Services	support@dbs.com	www.denabank.com

End user Module

In this module the end user can able to view the Cloud Storage Provider Details, Application Service Provider Details and Data Owner Details. The user can also Search for Content from the cloud storage and they can download the file by means of send request to the data owner to obtain the key to download the contents. The user can download the encrypted data from the cloud and use the decryption key.



UPLOAD CONTENT

S.No.

CS Provider Id

File Title

File Description

File Category

File

File S.No.

End User Id

From Date

To Date

Amount

Encryption Key

Decryption Private Key

File Details Saved.

IV. CONCLUSION

The existing system is describing the problem of secure authentication for storage in cloud. In this paper, proposed FA which carries out a flexible file-sharing scheme between an owner who stores the data in one cloud party and applications which are registered within another cloud party.

The security analysis shows that our N-FA (Novel Fuzzy Authorized) scheme provides a thorough security of outsourced data, including confidentiality, integrity and secure access control. Novel-Fuzzy Authorized approach reduces the storage consumption compared to other similar possible authorization schemes.

It also asserts that our scheme could efficiently achieve distance tolerance and realize fuzzy authorization in practice research study. This work mainly addresses the reading authorization issue on cloud storage. And it results to enable the TPA to perform audits for multiple users simultaneously and efficiently

REFERENCES

1. A. N.Khana, M. L.M. Kiaha, S.U. Khanb and S. A. Madanic, "Towards Secure Mobile Cloud Computing: A Survey", *Future Generation Computer Systems*, vol.29, Issues 5, July 2013.
2. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, *Above the clouds: a Berkeley view of cloud computing*, Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, Feb. 2009.

3. R. Ranjan, A. Harwood, R. Buyya, *Grid federation: an economy based distributed resource management system for large-scale resource coupling*, Technical Report GRIDS-TR-2004-10, Grid Computing and Distributed Systems Laboratory, University of Melbourne, Australia, 2004.
4. R. Buyya, R. Ranjan, *Federated resource management in grid and cloud computing systems*, *Future Generation Computer Systems* 26 (8) (2006) 1189–1191.
5. M. Al Morsy, J. Grundy and I. Muller, "An Analysis of The Cloud Computing Security Problem", In *Proceedings of APSEC 2010 Cloud Workshop*, Sydney, Australia, November 2010.
6. Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing," 2009, <http://www.wheresmyserver.co.nz/storage/media/faq-files/clouddef-v15.pdf>, Accessed April 2010.
7. Frank Gens, Robert P Mahowald and Richard L Villars. (2009, IDC Cloud Computing 2010.
8. J. Brodtkin, "Gartner: Seven Cloud-Computing Security Risks", Mar. 2009, Available at: <http://www.infoworld.com/d/security-central/gartnerseven-cloudcomputing-security-risks-853>.
9. Alliance for Telecommunications Industry Solutions. Homepage URL: <http://www.atis.org>.
10. Amazon S3 Availability Event: (2008). URL: <http://status.aws.amazon.com/s3-20080720.html> (Accessed on November 29, 2012)