Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.6, No.7, 2015

Framework to establish offline file sharing in Application as a service layer in cloud computing

Kajal Chachapara, and Prof. Rajesh Kumar Nigam (Associate Professor)
Department of Computer Science & Engineering,
Technocrats institute of technology, RGPV University Bhopal, India,

Abstract
Term cloud computing has opened entire new domain of computability, reliability and efficiency. Organizations can now focus on providing targeted services to consumers rather than considering infrastructure and resource issues. Cloud consumers can enjoy ease of computing and power of reliability but cloud service providers have to ensure many measures to let cloud services be reality and reliable. Consumers can store their valuable data on cloud and can use them as and when required. This leads to some key points like security of cloud data should be considered, sharing of cloud data as per requirement should be done. Allocation of required resources to the consumers should be done efficiently and above all, cloud service providers should have opportunity to gain some economical values. This research paper is based on providing some mechanism to allow file sharing among various cloud users. This paper proposed a framework that can be followed to easily share file residing on cloud with another cloud user. In this framework, concept of cryptography has been used to generate secure key that can be shared among users. Cryptography allows encryption and decryption of different normal text to some cipher text that cannot be interpreted easily. This paper has proposed secure mechanism of generating key, sharing a key and validating use of key for given file. Most important aspect considered in this research paper is, the user who owns a file and wants to provide access to other user don't have internet access at hand. Framework uses mobile technology to contact service providers and generate a key as and when needed.
Keywords— Cloud computing, cryptography, AES, RSA, Security, Authentication, Validation, Application as a service

I. INTRODUCTION

1.1. What is cloud?

Cloud computing is a computing paradigm that involves outsourcing of computing resources with the capabilities of expendable resource scalability, on-demand provisioning with little or no up-front the new economic model removes the need for the organization to invest a substantial sum of money for purchase of limited IT resources that are internally managed, but rather the organization can outsource its IT resource requirements to a cloud computing service provider and pay per use. However, organizational and institutional need for better value for money from their IT investments is the key factor driving cloud computing the survey provided important findings such as, the shift in the key drivers from cost to the need for IT resource scalability and flexibility.

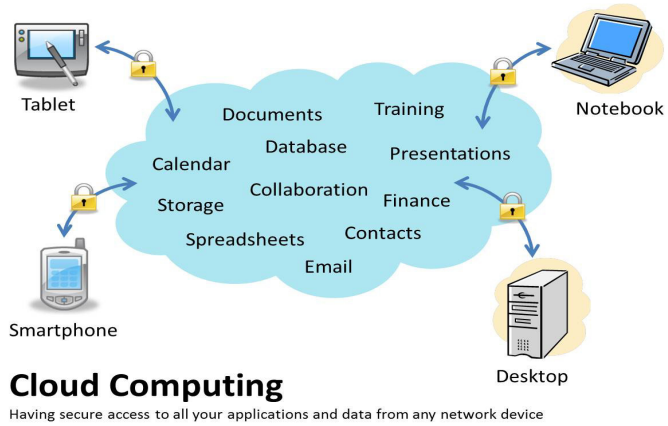


Fig.1 Basic cloud computing

As we can see infig.1 various network connected devices like smart phones, tablets, desktops and notebooks are using features of cloud computing with the help of internet connection. They can store their data like important documents, training data, calendar, finance and many more important documents. In such situation, secure mechanism of sharing and storage is essential considering advanced hacking techniques available now days.

1.2. Types of cloud

There are various types of cloud like private, public, community, personal, distributed and hybrid cloud. Private clouds are generally resources that are being used by single organization users within organizer. In private cloud all resources will be tightly secured and will be available within the organization. Public clouds are open cloud that any user can access with some credentials. User can also provide a link for their data to another user, if they wish. Google docs are simplest example of public cloud. I can put my documents on cloud and can use them on go. Hybrid clouds are combination of private and public cloud. Private cloud restricts sharing all over whereas public cloud provides full sharing. Current research work allows implementation of partial sharing in any type of cloud. Cloud providers can adapt proposed key generator to provide partial sharing functionality. Framework allows key sharing mechanism that is secure using cryptography algorithms. Organizations are adopting different types of cloud as per their document needs, security requirements and ease of sharing features.

1.3. Layers and security issues in cloud

Cloud computing seems really simple to the consumers of cloud as in access cloud, place or retrieve required data that's all. But internally cloud is built on three very important layers. Those layers are named as software as a service(Saas), Platform as a service(Paas) and Infrastructure as a service(IaaS). Various cloud service providers, provides different kind of services based on those layers. On first level that is software as services, various applications resides that provides interface to end users. This layer generally allows access to internal data with some authentication mechanism. Second layer is platform as a service, this layer contains various mappings of users request to the required resource that resides on cloud computing. At last there is infrastructure layer that is most time contains virtual machines and infrastructure that user can request for computations. Fig 2. Illustrates various layers of cloud computing pyramid.

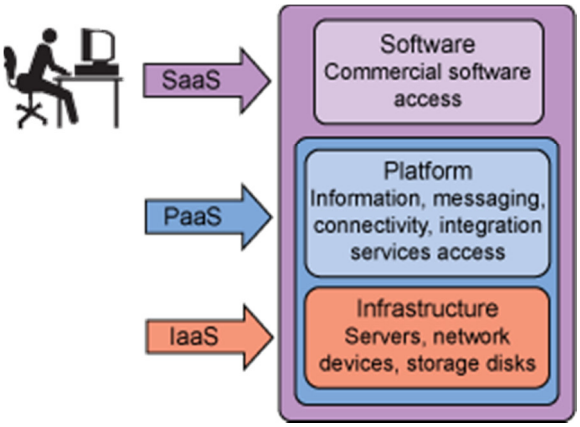


Fig.2 Cloud computing layers

Each layer of cloud contains its own vulnerabilities. Like software as a service layer uses authentication mechanism to validate owner's identity on document, but this can be broken if someone posses security code that is being used for authentication.

1.4. Cryptography

It is branch of security that proposes hundreds of algorithms that can be used for secure communication among various users or storing data securely on some media. This field provides methods for encryption, decryption and validation checks for different purpose. Encryption stands for converting simple plain text to some cipher text that is not easily understandable. Decryption performs reverse process of encryption for recover text from cipher text. Various approaches, algorithms can be adapted like AES, RSA, DES, Triple DES and various hashing algorithms like MD5 etc. it provides secure ways of generating key that can be used for encryption at sender side and for decryption at receiver side along with secure mechanism of transmitting those keys.

II. PREVIOUS PAPERS STUDY

In base paper [1], author has proposed privacy preserving authentication mechanism that will allow secure file access control on cloud. In system proposed cloud authenticates user without knowing their identities and allows them to store information. Authors have proposed mechanism that will prevent reply attacks.

In paper [2] proposed by Parsi Kalpana, Sudha Singaraju, Authors have verified various security issues and have proposed algorithm of generating key using RSA algorithm. Generated key will be further shared to communicate with cloud data. Particular file sharing mechanism is not provided.

In Literature survey, paper [3] proposed by Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou, allows defining access control policies based on attributes of data, meanwhile allows owner of file maximum control over data by providing maximum manipulations on file owners front. For processing they have used attribute based encryption, proxy re-encryption and lazy re-encryption.

There is also hierarchical attributes based encryption approach [4] in which company structure can be managed. In proposed system author have provided way of generating key at higher level and then passing that key to different levels of company structure that will be hierarchical. Higher level authority creates some access policies and keys and transfers them to lower level employees.

Based on literature study done, we figured out that in almost all proposed work authors have proposed mechanism of generating key, authenticating file owner of person asking for file access, revoking access provided. But authors have kept one requirement is owner of file must be online at the moment of generating key. Owner cannot generate key offline. Once key is generated, it can be distributed with different approaches but allowing key generation offline is challenge we have figured out in studies of various papers proposed in this area.

III. PROPOSED FRAMEWORK

This framework provides mechanism of secure file sharing among two users. Thus there will be some keyword or key notations that we will be using to explain how this framework will work. Below are some notations that we will use to explain framework functionality.
List of Keywords:

1. O(f) means owner of file.
2. R(f) means user who needs a file, generally it could be mobile no.
3. AT means secure Authentication Token of owner.
4. P means type of access permission that owner provides to requester on requested file like read, write etc.
5. UID means unique id of file, for which requester needs access.
6. Enc(data) means encryption of provided data.
7. Dec(data) means decryption of provided data.
8. C means number of times key can be used to access file.
9. To revoke generated key, file owner needs to contact service provider, need to provider access token and then provide key that should be revoked.

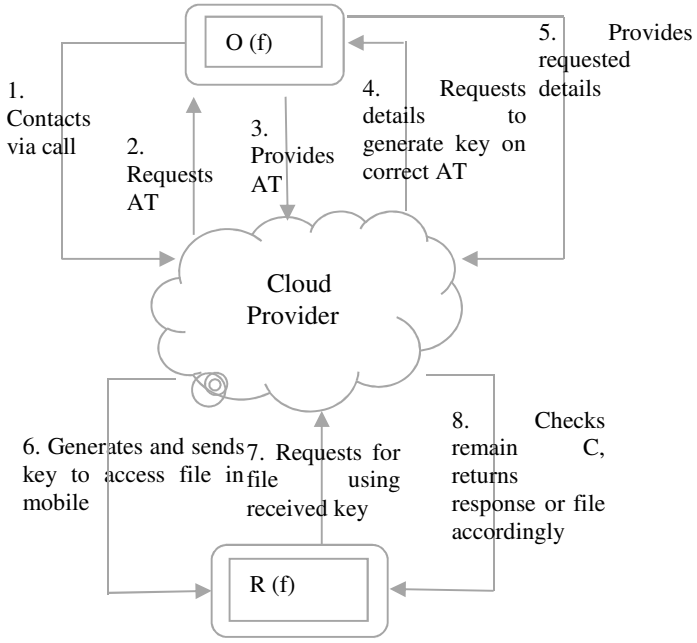


Fig.3. Proposed framework for secure link sharing

Explanation:

As given in fig.3, as a step1 owner of file will contact cloud service providers to generate link for selected file. When owner will contact cloud service providers via call, providers will ask for authentication token which is unique authentication password that will validate identity of owner. If authentication token is valid then service provider will return success with requesting details on file for which key needs to be generated. Once all details are available service providers will generate link containing selected access on selected file. Service provider will store C as count in some persistent storage available for further access validation.

Link = Enc(UID,P)

This link will be further passed to the mobile number provided by owner of the file as R(F). When R(F) will send request to cloud service provider on provided link. Based on link, first it will perform check of number of access done on said file using provided key, if number of access done are equal to that of provided by owner, service provider will simply return token with response as link expired. But if access counts are less that provided by owner then it will perform decryption of key using same algorithm used for encryption

Details = Dec(Link)

This decryption will provide unique id of file that has been requested, P as permission token that identifies as R for read, W for write and so on. Based on permission it will provide access to the requested file to requester and will update counter of access done in some persistent storage.

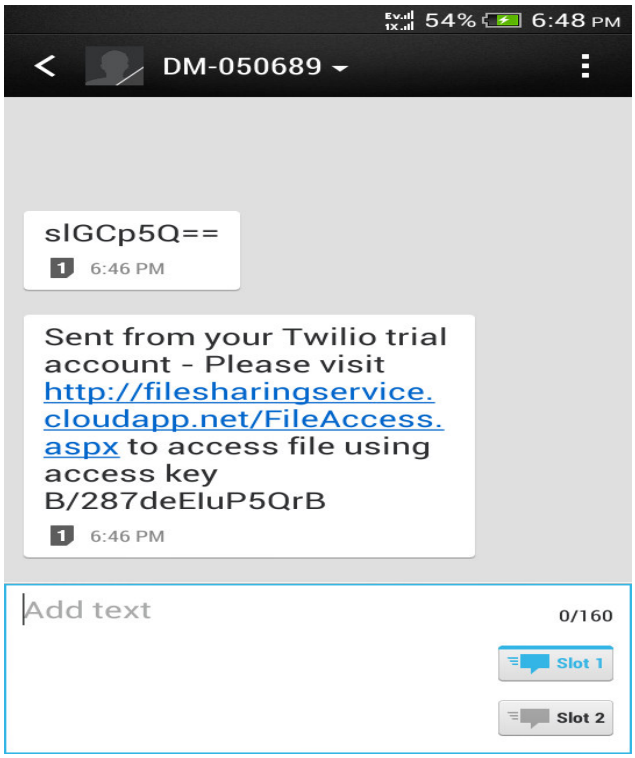
In any framework that allows sharing of important document, must provide revoke mechanism that will allow owner of file taking given access permission back. For this purpose we have proposed functionality of contacting cloud service provider via call again and provide them access token. Once token is verified service provider will ask for mobile number for which revoke operation needs to be done. Once owner of file provides it, key associate with that number will be disabled and user won't be able to access that file using that key.

IV. SIMULATION OF PROPOSED WORK

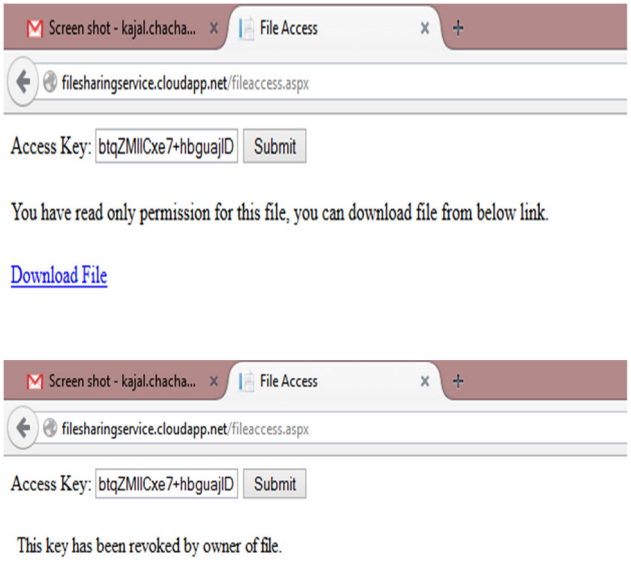
As per the key generation steps, first we will have to take a secret code from user, then we will generate 128 bit key using an AES algorithm. Then we will have to take a name of user for whom key is being generated and permission that we want to provide. Then we will merge details using formula defined in step 3 of fig.3. Final outcome will be encrypted again with RSA algorithm. Resultant key will be provided to user who can further

provide that key to another user.

Below is snapshot of SMS received containing security code along with link to follow!



User can get access to the file using that key, below is snapshot of how key can allow access to file



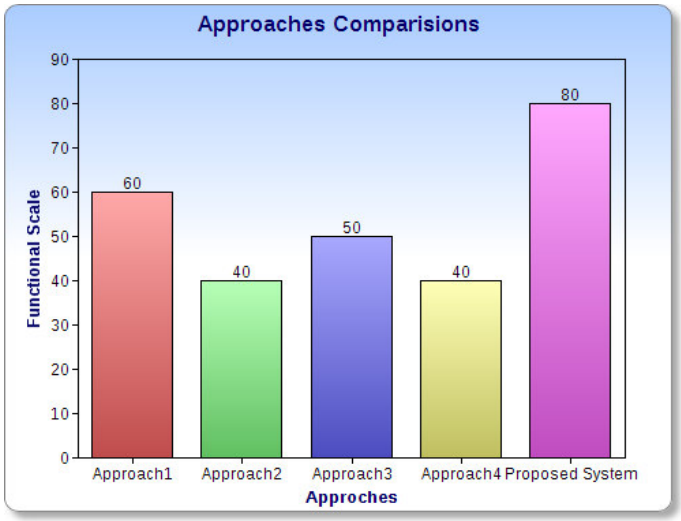
IV. COMPARISION WITH EXISTING APPROCHES

		[1]	[2]	[3]	[4]	Proposed System
Verifications, Controlling & Validations	Authentication	Y	Y	Y	Y	Y
	Authorization	N	Y	Y	Y	Y
	Revoke Mechanism	Y	Y	Y	Y	Y
Secure channels	Prevent reply attack	Y	N	Y	Y	Y
	Private public key encryption	N	Y	Y	N	Y
	Secure processing	N	Y	N	N	Y
Reliability & feasibility	File sharing	Y	N	N	N	Y
	Collision proof	Y	N/A	N	N	N
	Supports read write	Y	N/A	N	N	Y
	Work offline	N	N	N	N	Y

V. CONCLUSION AND FUTURE EXPANSION

In this research paper, we have tried to establish secure link sharing mechanism that will allow facility to cloud consumers sharing files without internet connection too. Being in larger organization, anyone can come across urgent requirement of document that is being owned by someone else who is on leave enjoying holidays on some hill station. In such circumstances, if such facility will be provided by cloud service provider then it will help them gain more economical value and win more satisfied consumers.

As per future expansion, we are planning to look for some attacks that can be done and break framework communication. We can work on this framework to make it more reliable & feasible for consumer requirements. Currently we have considered generating link of single file, same way we can work for more than one files. Also system is not collision proof. So we can implement taking copies and do modifications on that. We can also implement approval approach in which owner of file can approve updates on files.



VI. REFERENCES

[1].Sushmita Ruj, Milos Stojmenovic, Amiya Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing-2012.

[2].Parsi Kalpana, Sudha Singaraju, "Data Security in Cloud Computing using RSA Algorithm", International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012

[3].Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", Technical Program at IEEE INFOCOM 2010

[4].Guojun Wang, Qin Liu, Jie Wu, Minyi Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers.", Computers & Security 30 (2011) 320-331, 2011 Elsevier Ltd.

[5].Danan Thilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo, "Secure Data Sharing in the Cloud", S. Chen·S. Nepal CSIRO ICT Centre, Cnr Vimiera and Pembroke Rodas, Marsfield, NSW 2122, Australia

[6].Anurag Porwal, Rohit Maheshwari, B.L.Pal, Gaurav Kakhani, "An Approach for Secure Data Transmission in Private Cloud", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012

[7].M.Sudha , M.Monica, "Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography", Advances in Computer Science and its Applications 32 Vol. 1, No. 1, March 2012.

[8].Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem, "A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012

[9].Ahmad Rashidi and Naser Movahhedinia, "A Model for User Trust in Cloud Computing", International Journal on Cloud Computing: Services and Architecture(IJCCSA),Vol.2, No.2, April 2012

[10]. Dimitrios Zissis, Dimitrios Lekkas, "Addressing cloud computing security issues", Future Generation Computer Systems 28(2012)583–592

[11]. Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds, 2012 45th Hawaii International Conference on System Sciences

[12]. Ahmad Rashidi and Naser Movahhedinia, "A Model for User Trust in Cloud Computing", International Journal on Cloud Computing: Services and Architecture(IJCCSA),Vol.2, No.2, April 2012

[13]. Jianxin Li, Bo Li, Tianyu Wo, Chunming Hu, Jinpeng Huai, Lu Liu, K.P.Lam, "CyberGuarder: A virtualization security assurance architecture for green cloud computing", Future generation computer systems, 28(2012)379-390, 2011 Elsevier B.V.

[14]. Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", 2012 International Conference on Computer Science and Electronics Engineering

[15]. Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 201

[16]. D.H. Patil, Rakesh R. Bhavsar, Akshay S. Thorve, "Data Security over Cloud", International Conference on Emerging Frontiers in Technology for Rural Area (EFITRA) 2012 Proceedings published in International Journal of Computer Applications

[17]. Eman M.Mohamed, Hatem S. Abdelkader, "EnhancedData Security Model for Cloud Computing", The 8th International Conference on INFOrmatics and Systems (INFOS2012) - 14-16 May Cloud and Mobile Computing Track

[18]. Ronald Petrlic, Christoph Sorge, "Privacy-Preserving DRM for Cloud Computing", 2012 26th International Conference on Advanced Information Networking and Applications Workshops

[19]. Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2, FEBRUARY 2013

[20]. Nancy j.King, V.T.Raja, "Protecting the privacy and security of sensitive customer data in the cloud", SciVerse ScienceDirect, Computer Law & Security Review 28 (2012) 308-319

[21]. Ronnie D. Caytiles and Sunguk Lee, "Security Considerations for Public Mobile Cloud Computing", International Journal of Advanced Science and Technology Vol. 44, July, 2012

[22]. Kangchan Lee, "Security Threats in Cloud Computing Environments", International Journal of Security and Its Applications Vol. 6, No. 4, October, 2012

[23]. Abdul Nasir Khan, M.L. Mat Kiah, Samee U. Khan, Saijad A. Madani, "Towards Secure mobile cloud computing: A survey", Future generation computer systems,

[24]. Cong Wang, Qian Wang, Kui Ren, Ning Cao and Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing", IEEE Transactions on Cloud Computing Date of Publication: April-June 2012 Volume: 5 , Issue: 2

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar