International Journal of Computing Algorithm
Volume: 05 Issue: 01 June 2016, Page No. 17- 20
ISSN: 2278-2397

Smart Security For Data Sharing In Cloud Computing

Ayinavalli Venkata Ramana [1] B.V.Chaitanya[2] K.Indrasena Reddy[2] M.Venu Babu[2] V.Kavitha[2]
[1]Sr .Asstnt .Prof / Information Technology, GMR Institute of Technology, Rajam-Srikakulam District, A.P. India
[2] Student/ Information Technology, GMR Institute of Technology, Rajam , A.P ,India
Email: ramana.av@gmrit.org, rampraneeth.9@gmail.com, indrasenareddy.kundanam@gmail.com, mandangivenugmail.com, kavitha.vana222gmail.com

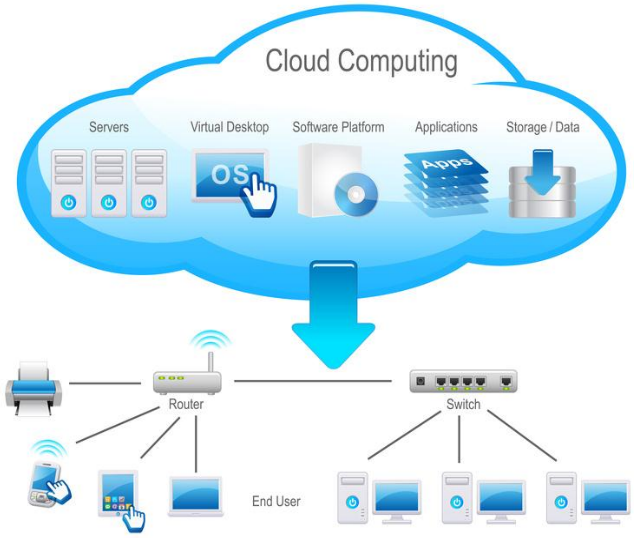
Abstract-- In these computational world security is the major Problem. Because the hackers are growing day by day. Here majorly attacker's attacks mostly while sharing or sending the data. So here we are using PAAS i.e. windows azure as the storage which is one of the service in cloud. So to provide the security for the data here we come up with an RSA (encryption and decryption) algorithm. This is one of the security mechanism to protect the private data over the cloud.

Index Terms— Cloud Computing, dynamic groups, data sharing, reliability, integrity, scalability.

I. INTRODUCTION

Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. Cloud computing is a comprehensive solution that delivers IT as a service. The flexibility of cloud computing is a function of the allocation of resources on demand. Before cloud computing, websites and server-based applications were executed on a specific system. Cloud computing is broken down into three segments application, storage and connectivity. cloud computing is completely real and will affect almost everyone. Changes in computer technology seem to move at lightning speeds. It wasn't that long ago that desktop computers had 20MB hard drives and people relied on floppy disks for storage. Now, cloud computing is shifting that computing power back to hosts again.

Only this time thing may different, because those hosts have become abstract, and are scattered all over the Internet. All over the world. That is to say that computing power is being shifted to the "cloud". Such a shift to cloud computing would not have been possible until now, because the enabling technology did not yet exist Broadband connectivity now makes cloud computing a realistic possibility for not just larger companies, but for small businesses, SOHO operations, and individual consumers. These users now have the fat pipes they need to access the cloud, and they also have access now to applications and services that they couldn't begin to access or afford just a few years ago. The possibilities are growing even faster as the US government undertakes its rural broadband initiatives, which in turn will push the potential of the cloud further to the masses. Today's emerging entrepreneurs can do everything over the Internet, and without the burden of huge up-front capital expenditures. According to the National Institute of Standards and Technology (NIST) Computer Security Division, the cloud model still suffers from significant security challenges. For example, Software as a Service (SaaS) vendors are implementing disparate security approach has, raising critical questions about where data is hosted, international privacy laws, exposure of data to foreign entities, nonstandard authentic teen and leaks in multi-tenant architectures. Cloud computing continues that trend by bringing greater levels of access to high-end applications and data storage, as well as new techniques for collaboration.



First, [1] cloud computing is an extremely broad term. It's as broad as saying "desktop computing" (i.e. the PC), which encompasses everything from the microchip to the Windows operating system to the software. As we will learn in this eBook, cloud computing encompasses all the same elements as the desktop. Second, you can't touch the cloud. Desktop computing is easy to understand because you can see, touch and feel your PC. The cloud is real, but it is abstracted to the point where you cannot see it, so it's harder to imagine. In reality, cloud computing encompasses other forms of computing beyond software, including the underlying hardware(infrastructure) and platforms. In many ways, cloud computing is strikingly similar to desktop computing in that it encompasses the same three basic elements: hardware (infrastructure), operating systems (platforms), and software. The main difference is that, with cloud computing, all three elements are "rented" over the Internet, rather than being managed locally.

II. PROBLEM STATEMENT

The cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task.

III. PROPOSED STSTEM

To solve the challenges presented above a secure multi-owner data sharing scheme for dynamic groups in the cloud. The main contributions of this paper include: This project proposes a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the un-trusted cloud. Proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and Computation overhead of encryption are constant and independent with the number of revoked users. Provide secure and privacy-preserving access control to users, which guarantee any member in group to anonymously utilize the cloud resource. Provide rigorous security analysis, and perform extensive to demonstrate the efficiency of scheme in terms of storage and computation overhead.

A. objective:

To implement an effective mechanism **f**or sharing of data in a multi owner manner in dynamic group in an untrusted cloud while preserving data and identity privacy.

B. Project Scope

The scope of the system is select the file from the system and it is to be send it to the other system which are in the cloud. After that we can transmitted the date with in as computer with the help of cloud.

C. Pr**oject Objective**

The system has a clear set of objectives to achieve. They are as follows:

1. Run all Group Manager
2. Select the File
3. Start sharing
4. Upload the File in the Clou

IV. SYSTEM SPECIFICATION AND ANALYSIS

A. Functional Requirements

The functional requirements are:

1. **Input**: Initial Input: Taking as a input file
2. Outputs: Encrypted file.

B. Non-Functional Requirements User interfaces and characteristics

Usability: Best GUI screens allow user to interact more effectively with limited knowledge on Data Mining.

Implementation: Using dot net (c#) and windows azure
Reliability: The system has ability to perform required operations under any conditions. This system is reliable and works effectively.
Performance: Performance requirements are concerned with quantifiable attributes of the system like response time and accuracy.

V. EXITING SYSTEM

The cloud, the group members can be completely released from the troublesome local data storage and maintenance. It also poses a significant risk to the confidentiality of those stored files. First, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Traceability, which enables the group manager (e.g., a company manager) to reveal the real identity of a user, is also highly desirable. Second, it is highly recommended that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner. Compared with the single-owner manner, where only the group manager can store and modify data in the cloud, the multiple-owner manner is more flexible in practical applications. More concretely, each user in the group is able to not only read data, but also modify his/her part of data in the entire data file shared by the company.

VI. PROPOSED SYSTEM

To solve the challenges presented above a secure multi-owner data sharing scheme for dynamic groups in the cloud. The main contributions of this paper include: This project proposes a [5]secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the un-trusted cloud. Proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and Computation overhead of encryption are constant and independent with the number of revoked users. Provide secure and privacy-preserving access control to users, which guarantee any member in group to anonymously utilize the cloud resource. Provide rigorous security analysis, and perform extensive to demonstrate the efficiency of scheme in terms of storage and computation overhead.

VII. ALGORITHM USED

The RSA algorithm is named after Ron Rivest, Adi Shamir and Len Adleman, who invented it in 1977. The basic technique was first discovered in 1973 by Clifford Cocksof CESG (part of the British GCHQ) but this was a secret until 1997. The patent taken out by RSA Labs has expired.

The RSA cryptosystem is the most widely-used public key cryptography algorithm in the world. It can be used to encrypt a message without the need to exchange a secret key separately. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers.

Party A can send an encrypted message to party B without any prior exchange of secret keys. A just uses B's public key to encrypt the message and B decrypts it using the private key, which only he knows. RSA can also be used to sign a message, so A can sign a message using their private key and B can verify it using A's public key.

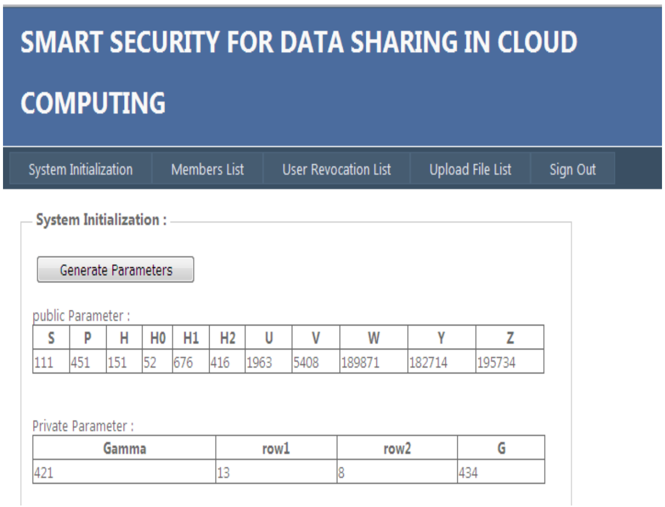
A. Key Generation Algorithm

- Required bit length, e.g. [2][3] Generate two large random primes, p and q, of approximately equal size such that their product n = pq is of the 1024 bits.
- Compute n = pq and (phi) φ = (p-1) (q-1).
- Choose an integer e, 1 < e < phi, such that gcd (e, phi) = 1.
- Compute the secret exponent d, 1 < d < phi, such that ed ≡ 1 (mod phi).
- The public key is (n, e) and the private key (d, p, q). Keep all the values d, p, q and phi secret. [We prefer sometimes to write the private key as (n, d) because you need the value of n when using d. Other times we might write the key pair as ((N, e), d).]

n is known as the modulus. e is known as the public exponent or encryption exponent or just the exponent. d is known as the secret exponent or decryption exponent.

VIII. RESULTS

The results are mostly based on group manager. He will be sending the data to the group members who got registered. So here the whole data that manager want to send to group member will be encrypted by using RSA algorithm. So the encrypted file can be send to the all users of groups i.e. there will be different groups in an organization where the manager if he is interested in sending the data to whole members then he can send it at once.


SMART SECURITY FOR DATA SHARING IN CLOUD COMPUTING

System Initialization :

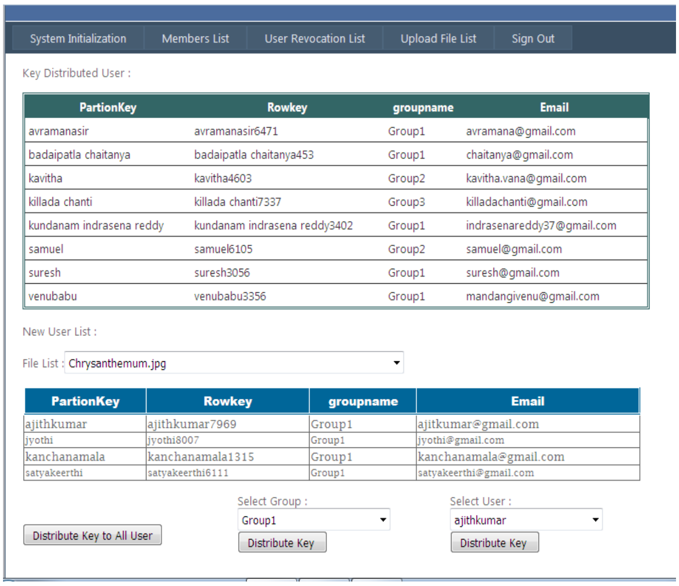
public Parameter :

S	P	H	H0	H1	H2	U	V	W	Y	Z
111	451	151	52	676	416	1963	5408	189871	182714	195734

Private Parameter :

Gamma	row1	row2	G
421	13	8	434

So everyone who are in that organization can get the total shared data in the encrypted format. Here by using the user's id the data will be getting encrypted and so the automatic link will be sending to the user when he will be login in to the site he will be getting accessed to the shared file. He can also have a way in sending the data to only particular group that he need to send or he can send the data to only single person that he need to go with. So the following are the screen shots of site in sending the data by group manager and the registration page of member who need to register.



Key Distributed User :

PartionKey	Rowkey	groupname	Email
avramanasir	avramanasir6471	Group1	avramana@gmail.com
badaipatla chaitanya	badaipatla chaitanya453	Group1	chaitanya@gmail.com
kavitha	kavitha4603	Group2	kavitha.vana@gmail.com
killada chanti	killada chanti7337	Group3	killadachanti@gmail.com
kundanam indrasena reddy	kundanam indrasena reddy3402	Group1	indrasenareddy37@gmail.com
samuel	samuel6105	Group2	samuel@gmail.com
suresh	suresh3056	Group1	suresh@gmail.com
venubabu	venubabu3356	Group1	mandangivenu@gmail.com

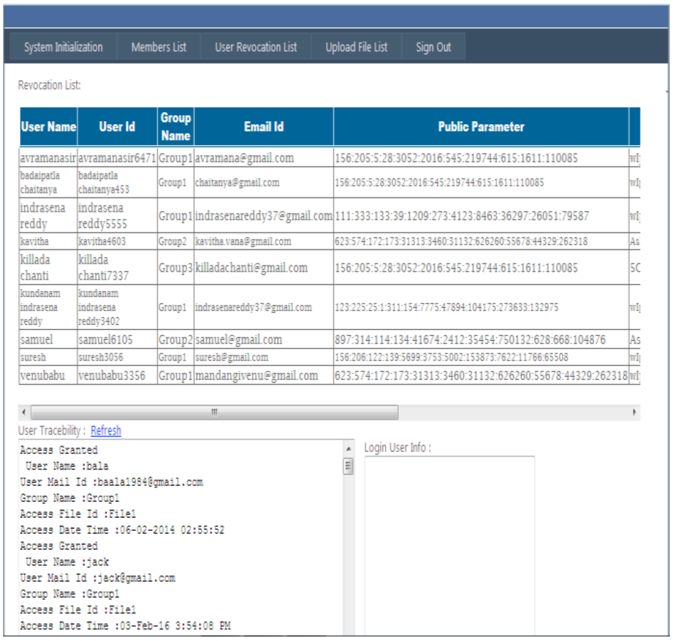
New User List :

File List : Chrysanthemum.jpg

PartionKey	Rowkey	groupname	Email
ajithkumar	ajithkumar7969	Group1	ajitkumar@gmail.com
jyothi	jyothi8007	Group1	jyothi@gmail.com
kanchanamala	kanchanamala1315	Group1	kanchanamala@gmail.com
satyakeerthi	satyakeerthi6111	Group1	satyakeerthi@gmail.com

Select Group : Group1

Select User : ajithkumar



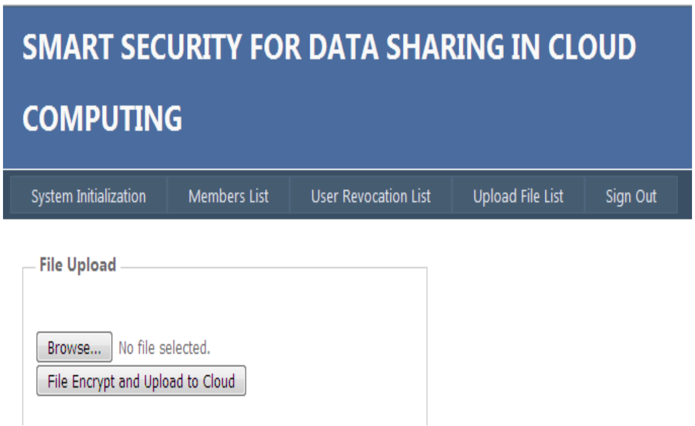
Revocation List:

User Name	User Id	Group Name	Email Id	Public Parameter	
avramanasir	avramanasir6471	Group1	avramana@gmail.com	156:205:5:28:3052:2016:545:219744:615:1611:110085	wl
badaipatla chaitanya	badaipatla chaitanya453	Group1	chaitanya@gmail.com	156:205:5:28:3052:2016:545:219744:615:1611:110085	wl
indrasena reddy	indrasena reddy5555	Group1	indrasenareddy37@gmail.com	111:333:133:39:1209:273:4123:8463:36297:26051:79587	wl
kavitha	kavitha4603	Group2	kavitha.vana@gmail.com	623:574:172:173:31313:3460:31132:626260:55678:44329:262318	As
killada chanti	killada chanti7337	Group3	killadachanti@gmail.com	156:205:5:28:3052:2016:545:219744:615:1611:110085	5C
kundanam indrasena reddy	kundanam indrasena reddy3402	Group1	indrasenareddy37@gmail.com	123:225:25:1:311:154:7775:47894:104175:273633:132975	wl
samuel	samuel6105	Group2	samuel@gmail.com	897:314:114:134:41674:2412:35454:750132:628:668:104876	As
suresh	suresh3056	Group1	suresh@gmail.com	156:206:122:139:5699:3753:5002:153873:7622:11766:65508	wl
venubabu	venubabu3356	Group1	mandangivenu@gmail.com	623:574:172:173:31313:3460:31132:626260:55678:44329:262318	wl

User Tracebility : Refresh

```
Access Granted
 User Name :bala
User Mail Id :baala1984@gmail.com
Group Name :Group1
Access File Id :File1
Access Date Time :06-02-2014 02:55:52
Access Granted
 User Name :jack
User Mail Id :jack@gmail.com
Group Name :Group1
Access File Id :File1
Access Date Time :03-Feb-16 3:54:08 PM
```

Login User Info :


SMART SECURITY FOR DATA SHARING IN CLOUD COMPUTING

File Upload

No file selected.

IX. CONCLUSION

Most of the work is related in providing security for the data while sharing between two or multiple groups. Here the manager will be sending the encrypted file to the individuals or group od all at once. So group members have to login in to the website and can access the data easily. Here the data will be in encrypted one so the user or member can access easily. So it is one of the way in providing security for data while sharing.

References

[1] http://www.springer.com/cda/content/document/cda_downloaddocument/9783642385858-c2.pdf?SGWID=0-0-45-1432954-p175259278

[2] A. Shamir, “Identity-based cryptosystems and signature schemes,” in CRYPTO. Springer, 1985, pp. 47–53.

[3] Abhijit Das, C. E. (2009). Public-Key Cryptography: Theory and Practice. Mumbai: Pearson Education India.

[4] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," *Comm. ACM*, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[5] Xuefeng Liu, Yuqing Zhang, Boyang Wang, Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE Transactions on Parallel & Distributed Systems, vol.24, no. 6, pp. 1182-1191, June 2013, doi:10.1109/TPDS.2012.331