Data Security over Cloud

D.H. Patil
Lecturer,Rajarshi Shahu
College Of Engg
Pune-33

Rakesh R. Bhavsar
Student, Rajarshi Shahu
College Of Engg.
Pune-33

Akshay S. Thorve
Student, Rajarshi Shahu
College Of Engg.
Pune-33

ABSTRACT

Data security and Access control is a challenging research work in Cloud Computing. Cloud service users upload there private and confidential data over the cloud. Security must be provided to such outsourced data, so that user are not worried while uploading there confidential data. Recent technologies suffer from computational problem of keys and there exchange. This paper addresses the various problems and issues involved in using cloud services such as key generation, data security, authentication. This paper addresses this problem using access control technique that ensures only valid users will access there outsourced data. This paper proposes a Diffie-Hellman key exchange protocol between cloud service provider and the user for secretly sharing a symmetric key for secure data access that solves the problem of key distribution and management. Authentication will be done using Two Factor Authentication Technique with the help of key generated using Diffie-Hellman key exchange algorithm The proposed work is highly efficient and secure under existing security models.

Keywords

Cloud Computing, Cryptography, Access Control, Security.

1. INTRODUCTION

Today’s most of small scale industries and companies are outsourcing there data over the cloud.Cloud is a infrastructure provided by the service provider to build internet application. Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a metered service over a network (typically the Internet)[2].Various commercial models are developed that can be described as “X as a service”, where X can be a hardware, software, application or storage. Various examples of cloud computing service providers are Google App Engine, Microsoft Azure, Amazon.

Cloud Computing however suffers from various security issues as data owners store their data on external servers, there have been increasing demands and concerns for data confidentiality, authentication and access control.Cloud providers have recognized the cloud security concern and are working hard to address it. In fact, cloud security is becoming a key differentiator and competitive edge between cloud providers. By applying the strongest security techniques and practices, cloud security may soon be raised far above the level that IT departments achieve using their own hardware and software. The work done proposes cryptographic access control model as shown in Figure.1 which we have considered as the system model in our work. This model mainly consist of Cloud Service Provider(CSP) and a Data Owner(DO).The Data Owner at first uploads the data over the cloud provided by the Cloud Service Provider. This data is kept in an encrypted format as the Cloud Service Providers may not be trustworthy. Then whenever the data user requiresthere data, authentication occurs and data access is provided to valid users if the authentication is successful. This is shown in the following figure 1.Some methods of data security guarantees confidentiality, integrity and authentication, but the problem with this model is that the owner is required to be always online when the user wants to access the data. The key management between the Data Owner and Cloud Service Provider is also very difficult.

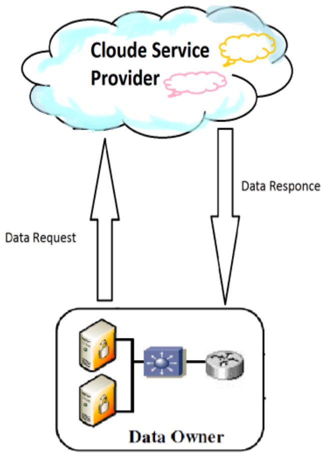


Figure 1: Example of Secured Data Access

We proposed a secure and efficient data access to the cloud service users. The proposed system ensures secure access to outsourced data. It also relieves the DO from worrying about data access request made by the user, resulting in increase efficiency of access control

2. LITERATURE SURVEY

While coming with this paper we had visited many small scale industries and companies those are recently using cloud services for outsourcing there confidential data over the cloud and are suffering with some problems while exchanging keys and accessing the services. They are also worried about the recent security techniques, which are currently available. For this paper we have refer the technical paper on Secure Data Access Over Cloud Computing And Secure Data Access In Cloud Computing. With the help of these two papers we are providing a combined approach for providing security over the cloud, which mainly consist of using a Diffe-Hellman Key Exchange Protocol and Two Factor authentication technique.

For data security, the user data will be outsourced in an encrypted format using a RSA algorithm.

3. SYSTEM ARCHITECTURE

In our proposed system we are developing two parts, namely Data owner and cloud service provider. Data owner is our user and the Cloud Service Provider is a Combination of several Service providers like Amazon, Google, and Microsoft which has very large storage and computation capacity. Cloud Service Provider is always online. The authentic users can get theredata file that is stored on the Cloud whenever they requires. We also assume that Data owner is not always online. We also assume that the Data Owner can also execute a binary application code at the Cloud Service Provider for managing his data files. Communication between the Data owner and Cloud Service Provider is made secure using cryptographic algorithm like Diffie-Hellman Key Exchange and symmetric Key Encryption. Diffie-Hellman key exchange algorithm is used to exchange the key between Data Owner and Cloud Service Provider, which removes the dis-advantages of current technologies where there is heavy load and overhead in Key Distribution Management.Data owner creates their accounts on the cloud. Cloud service provider maintains the list of its entire user by registering them into database. While registering the user or data owner is required to provide there user id and password and some other User information details and a entry is made into database. This entry contains the information about data owner, its username and mobile number.User mobile no.is used for cheeking whether the user is genuine or not by sending him a message which will contain a password generated using the Diffie-Hellman Key Exchange Algorithm. This password then user enters which after matchingwith the one generated by the server a account is being created. After creating the account on cloud, data owner can use the services that are provided by the cloud service provider.

We use two-way authentications for accessing the account. When users wants to login into their account, after entering the username and static password, another one time password is sent to the user on their specified mobile number by server. Using this password user can login into their accounts. One time password lasts for the complete session or for given time slice. Before transferring any data files to the cloud user encrypts them with a symmetric key which ensures that the data is secured and can not be read by anyone and even if the data is being hacked or stolen will be of no use to that person or a hacker. We use symmetric key algorithm for encryption and decryption of user data. These symmetric keys are generated and exchange using Diffie-Hellman algorithm. Using that symmetric key user can secure their private data from being lost. In this way over proposed scheme removes the dis-advantages of the Data Owner being always online and it also removes the dis-advantage of overhead in Key Distribution Management.

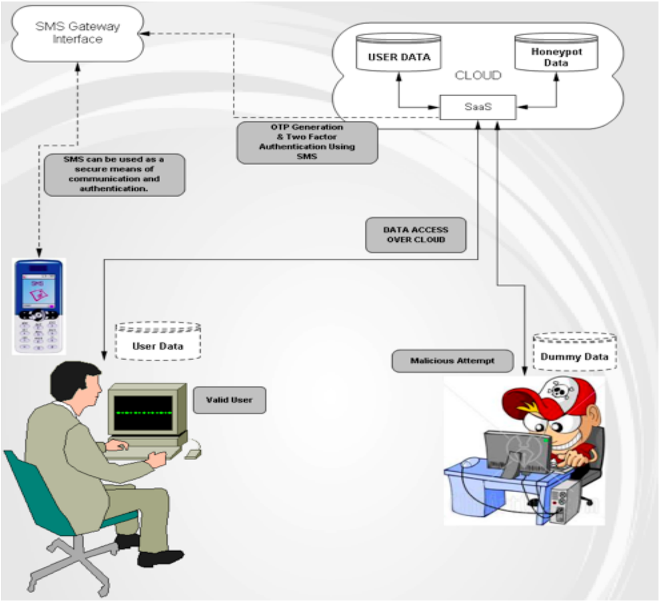

SMS Gateway Interface
USER DATA
Honeypot Data
CLOUD
SaaS
OTP Generation & Two Factor Authentication Using SMS
SMS can be used as a secure means of communication and authentication.
DATA ACCESS OVER CLOUD
User Data
Valid User
Malicious Attempt
Dummy Data

Figure 1: **System Architecture**

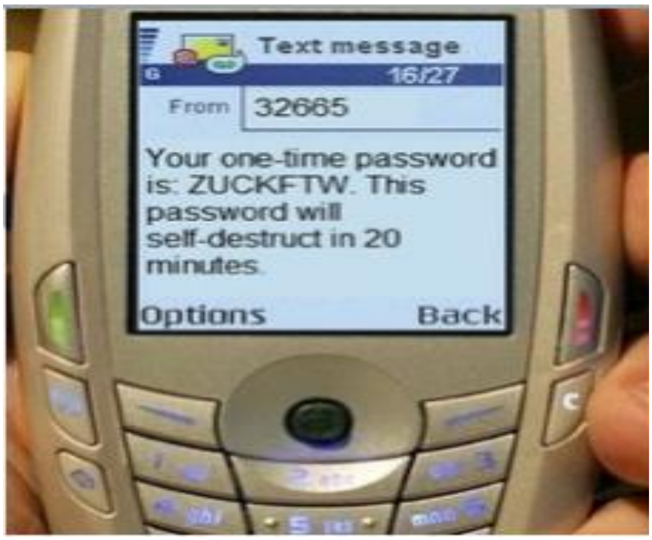
4. FUNCTIONAL SPECIFICATIONS

A. AuthenticationModule:

1) Make New Registration for Cloud Service
:At first the company or a user who needs the various cloud services are required to register. During registration various details of user such as there user id and mobile no. is taken . The mobile no.is later used for validating a user whether it is a genuine user or not by sending immediately a small text message which will include a key that the user will require to enter for creating a account over the cloud and then the registration will be successful. Figure shows how the authentications process occurs which depicts that when a user enters its user id and a password, a key is being send to his device which is being generated using a D-H Key Exchange and also this key is valid a specific time instance and will get destroyed after that specific time instance.

2) Using Cloud Service:
Whenever a user is required to use the services provided by the cloud service provided ,the user enters his user id and password ,if the user id and password is correct a new key is generated using the Diffie-Hellman Key Exchange Algorithm and is sent to the users mobile device using the number which was provided by the user during registration.

The user then enter the key which he/she has received onhis device .If the key matches with the one generated using the Diffie-Hellman Algorithm, data access is provided to the user and all the cloud services are provided to the user after authentication is made successful.



From 32665

Your one-time password is: ZUCKFTW. This password will self-destruct in 20 minutes.

***Figure 1:* Authentication Module**

B. Administrator Module

Administrator Module is mainly used for User database management that will be used bye the cloud service providers for providing specific services to specific users only. It will also be used for deciding the various access rights for different users as per their login details. For example say Company Owner will be provided all the rights and their employees according to the access rights provided by the company owner.

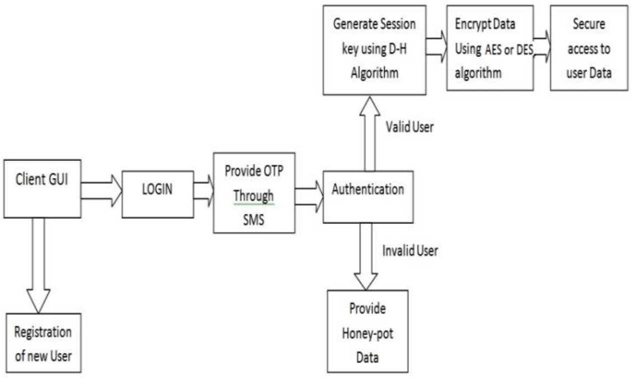


Figure *1:* Block Diagram Of a System

C. Encryption and Decryption Module:

The data which the user will outsource over the cloud will be kept in an encrypted format using the same key which was generated using the Diffie-Hellman algorithm. This encryption will ensure that even if the data is being hacked or is been seen by some one, then it will be in an encrypted format and will be of no use to the unknown person who has stolen that data. Similarly the Decryption process will occur if the user is genuine and the data access will be provided only to the valid uses. In this way the encryption and Decryption module will also provide a security to the outsourced data and will be secured.

5. ANALYSIS OF OUR PROPOSED SCHEME

Security Analysis:

Inthis section, we analyze the security properties and the performance of our Proposed Scheme. The analysis consist of analyzing various security properties such as Data Confidentiality, Authentication and Integrity of the data.

1) *Data Confidentiality:* Data Confidentiality of our proposed scheme is analyzed by comparing it with various data Encryption algorithms such Advanced Encryption Standard or Data Encryption Standard which uses the symmetric key for encrypting the data.

In our proposed scheme as the data is encrypted, hence the cloud service provider do not have any access to the data as he do not know the key, and is only known to the data owner which ensures the Data Confidentiality.

2) *Authentication*: In our proposed scheme, whenever a new user is added or it tries to access the data over a cloud , a Two Factor Authentication is performed with the help of the password set by the user during registration and the key which is generated with the help of Diffie-Hellman algorithm which is sent to the user mobile device. If the password and the key matches or is correct then access is granted to the user over the cloud services. In this way the Authentication occurs in our proposed scheme.

3) *Integrity*: Integrity of data is maintained with the help of encryption module of our proposed scheme. It ensures that the data integrity is maintained and the data over the cloud is secured.

4) *Computational Complexity*: Fig shows the computational complexity of a public key encryption technique and the Diffie-Hellman Key Exchange. As the size of the Key increases, the computation complexity also increases in the Public key encryption technique when compared to Diffie-Hellman Key Exchange.

This shows that the computation complexity of a Diffie-Hellman Key Exchange is much better as compared to any Public key Encryption technique.

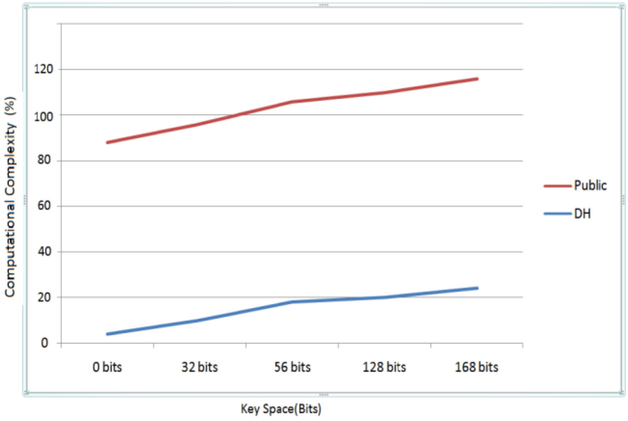
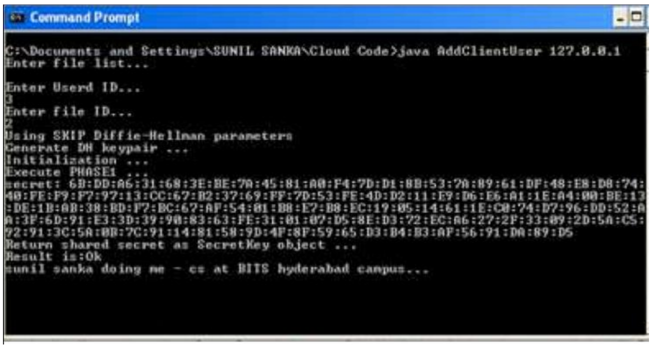


Figure : Computational Complexity Of D-H and Public Key

6. SIMULATION

In this section, we describe our simulation of our system. Servers and clients are created using Java RMI technique. We set up the Cloud Server on one machine and Data Owner Server on another machine. These machines are having specifications as-Intel[R] Core 2 Duo CPU with the speed of 2.90GHz having 1.96 GB of RAM. Both the machines were running Microsoft Windows XP, Service Pack 2 Operating System. Java RMI methods of remote Java objects can be invoked from other Java virtual machines, possibly on different hosts. The Data Owner has the flexibility to come online at any time which removes one of the dis-advantages of always Data Owner being online. Data Owner can make any changes to data files stored by them. We ran all our processes for all possibilities and got observable result.



```
C:\Documents and Settings\SUNIL SANKA\Cloud Code>java AddClientUser 127.0.0.1
Enter file list...

Enter Userd ID...
3
Enter file ID...
2
Using SKIP Diffie-Hellman parameters
Generate DH keypair ...
Initialization ...
Execute PHASE1 ...
secret: 6B:DD:A6:31:68:3E:BE:7A:45:81:A0:F4:7D:D1:8B:53:7A:89:61:DF:48:E8:D8:74:
40:FE:F9:F7:97:13:CC:67:B2:37:69:FF:7D:53:FE:4D:D2:11:E9:D6:E6:A1:1E:A4:00:BE:13
:DE:1B:AB:38:BD:F7:BC:67:AF:54:01:B8:E7:B8:EC:19:05:14:61:1E:C0:74:D7:96:DD:52:A
A:3F:6D:91:E3:3D:39:90:83:63:FE:31:01:07:D5:8E:D3:72:EC:A6:27:2F:33:09:2D:5A:C5:
92:91:3C:5A:0B:7C:91:14:81:58:9D:4F:8F:59:65:D3:B4:B3:AF:56:91:DA:89:D5
Return shared secret as SecretKey object ...
Result is:Ok
sunil sanka doing me - cs at BITS hyderabad campus...
```

***Figure 4*: Implementation of Diffie-Hellman Key Exchange**

7. ADVANTAGES AND BENEFITS

1. A good control over the business assets. The main assets in any company are its data files with customer information.
2. Risk of data loss due to improper backups or system failure can be avoided.
3. Security, Privacy, Compliancy along with availability is achieved.
4. Data Owner is not required to remain always online whenever a user is required to use services provided bye the Cloud Service Provider.

8. FUTURE SCOPE

1 Sharing of a software's over various types of network such as LAN/MAN/WAN/Internet in a secured way.

2 The ability to make software sharable and the client PC acting as a dump terminal opens up a new concept over a software industry i.e Virtualization of Software's

3 Enabling user to use different types of features provided by various software in a secured manner.

4 There will be no any type of attack or data loss caused by the attackers and the intruders.

5 A very high security will be provided to the users who outsourced there data to the cloud service providers and thus the use cloud services will be increased tremendously.

5. Enables new Business opportunities such as:
A} On- Demand IT
B) Self-service IT
C) Pay By Use.

9. CONCLUSION

This paper represents the security methods, which secure the data of users not only at the cloud but also on transmission as the man in middle attack is completely avoided by Diffie-Hellman key exchange algorithm. This paper also addresses the problems of the access control using proper authentication mechanism by two factors. D-H protocol fits better in this scenario as number of users on cloud is very large and key management is very difficult. Our proposed scheme eliminates the overheads of key computation and their management. Implementation of the cryptographic algorithms in a cloud computing environment using Java RMI is also covered in this paper. Provision of security to the users data on the cloud will defiantly empowers the Data owner to outsource the data to cloud.

10. REFERENCES

[1] Eoin Gleeson, "Computing industry set for a shocking change," Apr 2009, MoneyWeek, from http://www.moneyweek.com/investment-advice/computing-industry-set-for-a-shocking-change-43226.aspx

[2] "The NIST Definition of Cloud Computing". National Institute of Science and Technology. Retrieved 24 July 2011.Mudili Soujanya, Sarun Kumar,*Personalized IVR system in Contact Center, Department of Computer Science Engineering* International Institute of Information Technology Bhubaneswar, India.

[3] Reza Sherafat Kazemzadeh and KamranSartipi, *Incoporating Data Mining Applications into Clinical Guildelines*, McMaster University Department of Computing and Software 1280 Main Street West, Hamilton, Ontario, Canda.

[4] S. Kamara, and K. Lauter, "Cryptographic Cloud Storage," in Proc. of Financial Cryptography: Workshop on real life cryptographic protocols and standardization, 2010, from http://research.microsoft.com/pubs/112576/crypto-cloud.pdf

[5] Amazon EC2 and S3, Online at http://aws.amazon.com/

[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," in Proc. of IEEE INFOCOM 2010, 2010.

[7] Z. Dai, and Q. Zhou, "A PKI-based Mechanism for Secure and Efficient Access to Outsourced Data," in Proc. of International Conference on Networking and Digital Society, 2010, pp. 640-643.

[8] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," in Proc. of IEEE INFOCOM 2010, 2010.

[9] L. M. Vaquero, L. Rodero-Merino, J. Caceres, M. Lindner, "A Break in the Clouds: Towards a Cloud Definition," in Proc. Of ACM SIGCOMM Computer Communication Review, 39(1), Jan 2009, pp. 50-55.