Design of Secure Authenticated Key Management Protocol for Cloud Computing Environments

CHALLA RAVI TEJA [#1], K.RAMBABU [#2]

[#1] MSC Student, Master of Computer Science,
D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.
[#2] Head & Assistant Professor, Master of Computer Applications,
D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

ABSTRACT

In current day's cloud computing has become one of the fascinating domains which are used by almost all MNC and IT companies. Generally this is formed by interconnecting a large number of systems connected all together for remote servers hosted on internet to store, access, retrieve data from remote machines not from local machines. In present days there was no security for the data which is stored in the cloud server, because the data is not encrypted by strong means of encryption and there is no facility to block the user revocation. In order to address the issues related to data security and user revocation in the public network, we try to design a three-factor Mutual Authentication and Key Agreement (MAKA) protocols for achieving those two concepts. Here in this current paper we try to address these limitations of current cloud server and we propose a provable dynamic revocable three-factor MAKA protocol that achieves the user dynamic management in which if any revoked user want to access the cloud sever cannot able to access the cloud with his old credentials. By conducting various experiments on our proposed method, simulation results clearly state that proposed method is best in providing security against data revocation under distributed storage environment.

Keywords

Cloud Computing, Revocation, Mutual Authentication, Key Agreement, Encryption, Decryption, Dynamic Revocable

1. INTRODUCTION

Cloud computing will generate a lot of computation space and storage capacity to store and access the information to and from the remote locations. This will greatly attract different types of clients (I.e. Mobile Phones, Personal Computers, Automation Companies) to store and access the information from remote locations with their individual requirements and comforts. Among various instances gave by cloud computing, cloud storage administration, for instance, Apple's iCloud, Microsoft's Azure, DriveHQ, Silicon House offers a progressive approach to share the information over the internet, by providing a lot of

advantages for the general users. Almost in all the cases the cloud domain is facing a lot of security problems occurred by the intruders. Furthermore, information sharing is mostly exposed in open environments with very poor security and therefore the cloud server would become an objective of assaults.

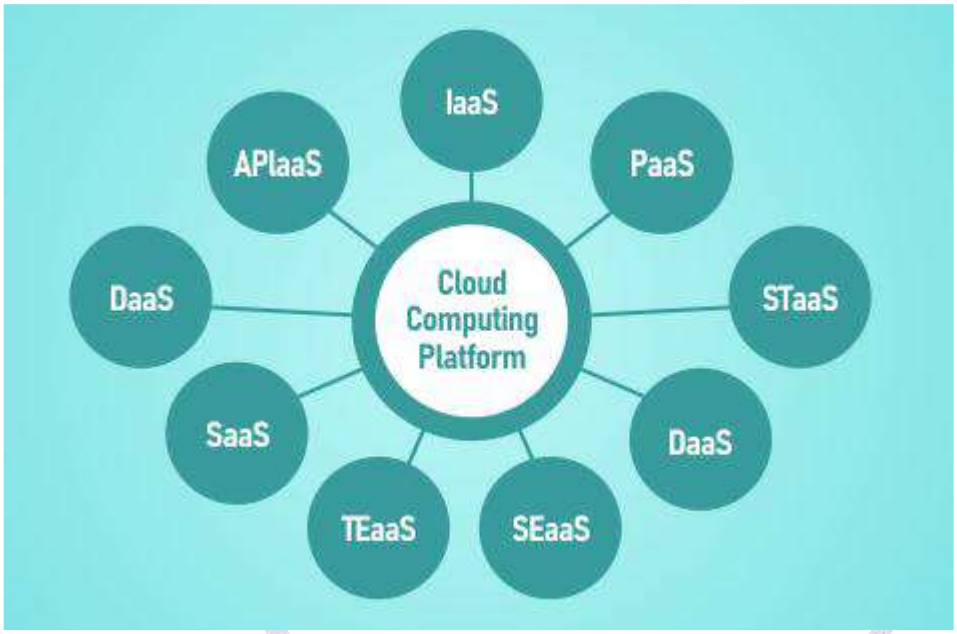


Figure. 1. Represents the Several Cloud Services in Real World Environment

In a recent survey we came to know that most of the information from cloud server is revealed by the users who are directly associated with internal server. These internal users may expose the valuable client's information to third party persons who are eagerly waiting for that information. As we know that some users will be terminated from their roles due to some personal cause or under termination process, the key access which is given for that terminated user will not be blocked immediately by the cloud server, hence the user can illegally try to access the same information from outside and gain the valuable information. Hence this process should be dynamically identified and block such revoked users not to access the server with their current credentials. One solution to overcome this problem is to use the cryptography method to include identity based encryption (IBE) to access this security. Here the term identity means the access permissions will be dynamically changes for user periodically and based on user preference only, he/she can able to access the data from the cloud server.

From the above figure 1, we can identify there are lot of cloud services present in the real time environment and out of all those services one will mainly discuss about the four types of services like:

1. IaaS,
2. PaaS,
3. SaaS and
4. DaaS.

One among the best service is DaaS, in which this DaaS is mainly used for storing and accessing the sensitive information from different clients who are connected to remote servers for storing the sensitive

information and try to provide access for the requested users. In current days this is not having proper security hence in this proposed thesis we try to provide security for this DaaS service by using primitive cryptography technique and by using an secure protocol known as MAKA for efficient key management and multi authority environment technique.

2. LITERATURE SURVEY

Literature survey is that the most vital step in software development process. Before developing the tool, it's necessary to work out the time factor, economy and company strength. Once this stuff is satisfied, ten next steps are to work out which OS and language used for developing the tool. This literature survey is mainly used for identifying the list of resources to construct this proposed application.

MOTIVATION

A well-known author. Leslie Lamport [6] has written a paper on"Password authentication with insecure communication". In this paper the authors concentrated more on the cloud computing and also about the most important features of the cloud. In general a new method for user password authentication is discussed which is more secure even if an intruder try to read the systems data. The proposed method can able to identify a one-way encryption function and can be implemented using a small micro devices to control and monitor the user need.

A well-known author Sherali Zeadally [7], has written a paper on" An Enhanced and Provably Secure Chaotic Map-Based Authenticated Key Agreement in Multi-Server Architecture". In this paper the authors mainly concentrated on the problem of building and establishing a secure cloud server on the top of all public cloud infra structures. They mainly identified the high level security preference and also about the recent cryptographic primitives. The authors mainly concentrate on the cryptography techniques which were used for providing security for the data encryption and decryption. Here the authors conducted a survey on cloud and its importance in public storage area.

A well-known author Azeem Irshad [8], has written a paper on "An Enhanced and Provably Secure Chaotic Map-Based Authenticated Key Agreement in Multi-Server Architecture". In this paper the authors mainly concentrated about the In the multi-server authentication (MSA) paradigm, a subscriber might avail multiple services of different service providers, after registering from registration authority. In this approach, the user has to remember only a single password for all service providers, and servers are relieved of individualized registrations. Many MSA-related schemes have been presented so far, however with several drawbacks.

3. THE PROPOSED SECURE AUTHENTICATED KEY MANAGEMENT PROTOCOL FOR STORING THE DATA UNDER DATA REVOCATION

In this proposed thesis we try to design an idea called MAKA PROTOCOL : Mutual Authentication and Key Agreement Under data revocation for constructing a financial support which can be satisfied by all the primitive objectives.

Here we try to address some formal definitions to MAKA algorithm and try to concentrate more about its security. We try to discuss more about the implementation of RS-IBE algorithm and its advantages. The proposed security model is mainly proposed or designed based on the standard model like the decisional ℓ-Bilinear Diffie-Hellman Exponent (ℓ-BDHE) supposition. In other words we can say that proposed scheme can give more security for the encoding and decoding of user authentication.

The proposed technique is best in following ways like : this can provide secrecy of data in both forward and backward methods. The primary role of this proposed plan is all the data will be initially converted in plain text manner before it is stored into the server location.

As the data is stored in an encrypted manner for accessing the file, the user needs the access permission from the cloud server. This access permission will try to restrict un-authorized users.

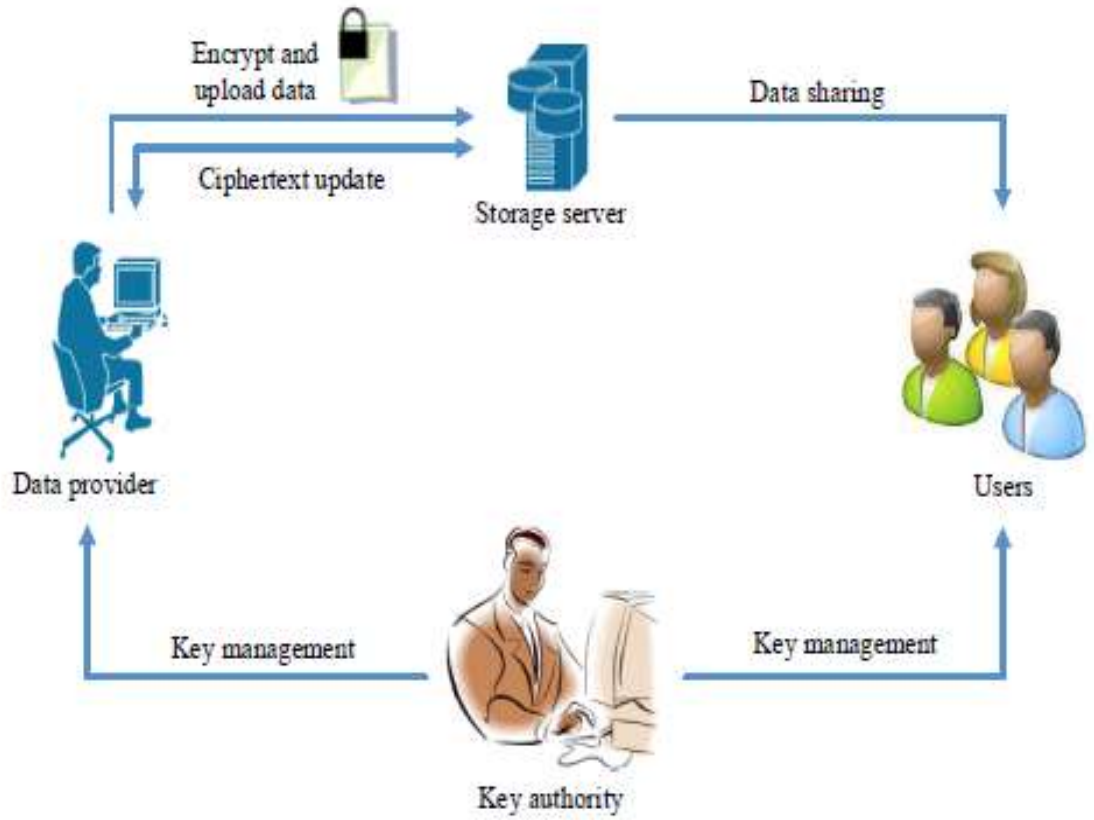


Figure. 2. Represents the Proposed MAKA Protocol Under Data Revocation

One main characteristic of the proposed approach is the cipher text which is converted need to have the access permission like read/write and then post those encryption plans on that and at the end we need to calculate the parameter's like: the calculation and capacity unpredictability, which are presented in by the mystery, is all upper limited by O (log (T) 2), where T is the all-out number of services.

From the above figure 2,we can clearly identify the proposed MAKA protocol has the following 4 entities like:

1. Data Provider
2. Data User
3. Storage Server and
4. Key Authority

Once the application is started the data owner and data user need to register first into the application with all the basic details. Once they get registered now the data owners and data users will get authorization from storage server that they can login and perform their individual operations. At this stage the data owner can able to login and upload the file into the storage server. As we all know that in current days the data which is uploaded into the cloud server will always be stored in plaintext manner, for a security purpose we try to encrypt the data and then store the encrypted documents in to the storage location. Here we try to apply a advanced encryption technique like revocable storage identity based encryption (RS-IBE) algorithm

for encrypting the data and storing the parameters in the centralized server location. As we use RS-IBE for encrypting the data the keys are controlled by the key authority which is present in our application. If any data user who want to access the file in plain text manner then that user need to request the key authority for granting key permissions and then only the data can be opened in a plain text manner.

During the process of data upload and data download, if any user who forget to substitute the keys wrongly provided by the key authority, then the user will become as revoked user and such a user cannot able to access the files which he is having permission to access earlier.This is because of the reason like revoked users are blocked by the MAKA protocol and those who are present in active state only can access the files from the cloud server and remaining all cannot able to access the file blocks from the cloud server. If this was implemented in current cloud environments we can achieve much more security for the data which is stored and accessed from the cloud server.

4. IMPLEMENTATION PHASE

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. The front end of the application takes JSP,HTML and Java Beans and as a Back-End Data base we took My SQL data base. The application is divided mainly into following 4 modules. They are as follows:

1) Data Provider
2) Storage Server /Cloud Server
3) Key Authority
4) Data User

Now let us discuss about each and every module in detail

1. DATA PROVIDER MODULE

The data provider is one who try to register into the application and once he gets registered he can able to login into his account and he can do following operations like :

1. He can able to upload the sensitive documents
2. He can encrypt the data by using secret key
3. He can request key from Key authority
4. View Key request from Data user
5. Allow or Deny key request of data user
6. See history of data users

2.STORAGE SERVER MODULE

Here the storage server is nothing but cloud in which this will try to hold all the sensitive information in a secure manner. The storage server has the following facilities likes:

1. View Storage Server Files
2. View End user and View Owners
3. View Secret Keys
4. View Attackers
5. Unblock Revoked Users
6. View Transactions
7. View Results in Chart manner

3. KEY AUTHORITY MODULE

Here the key authority is third party auditor which is used to grant keys and permissions for the data owners and end users. This will also has the facility to restrict the un-authorized users not to access the cloud data. This Key authority once getting login into its account, it has following operations like:

1. Generate Secret Key
2. View End users and their request
3. View Attackers

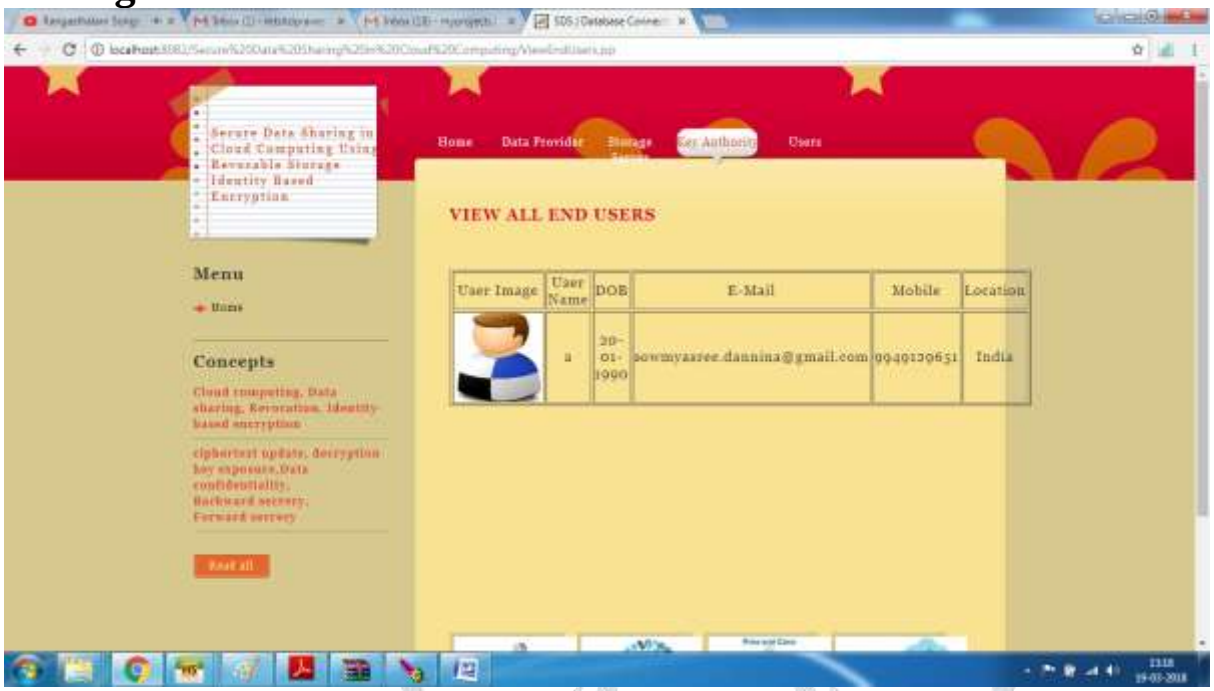
4. DATA USER MODULE

The data user is one who can able to register into the application with all his basic details and once he/she gets registered he will be able to do following operations:

1. Request Secret Key from Service Provider
2. View Secret Key that is generated by Key Authority
3. Download the Data in a plain text manner
4. Verify whether as genuine user or Attacker

5. EXPERIMENTAL REPORTS

Storage Server can see the list of end users who are available in the server



User try to login with his user credentials

User can request secret key after his login for the file which he want from owner

User gets the key from the owner or service provider

User download the data by substituting keys correctly

If the user substitute the key or file name wrongly he will be revoked

6. CONCLUSION

In this paper we for the first time designed and developed a novel algorithm like MAKA PROTOCOL, which can update the information dynamically in the cloud server, and try to fix the user's access permissions. Here the client or user data approval about information should be dynamic if at all when the approval gets lapsed and should be revocable. Hence we try to propose RS-IBE algorithm, where approval is refreshed efficiently and all the while. The exhibition of the proposed (RS-IBE) has focal points regarding usefulness and effectiveness. By conducting various experiments on our proposed method,

simulation results clearly state that proposed method is best in providing security against data revocation under distributed storage environment.

7. REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.

[2] iCloud.(2014) Apple storage service.[Online]. Available: https://www.icloud.com/

[3] Azure.(2014) Azure storage service.[Online]. Available: http://www.windowsazure.com/

[4] Amazon.(2014) Amazon simple storage service (amazon s3). [Online]. Available: http://aws.amazon.com/s3/

[5] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," Services Computing, IEEE Transactions on, vol. 5, no. 4, pp. 551–563, 2012.

[6] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.

[7] G.Anthes, "Security in the cloud," Communications of the ACM, vol. 53, no. 11, pp. 16–18, 2010.

[8] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.

[9] B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in INFOCOM, 2013 Proceedings IEEE. IEEE, 2013, pp. 2904–2912.

[10] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 384–394, 2014.

[11] X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, "Cost-effective authentic and anonymous data sharing with forward security," Computers, IEEE Transactions on, 2014, doi: 10.1109/TC.2014.2315619.

[12] C.-K.Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 468–477, 2014.