Secure open cloud in data transmission using reference pattern and identity with enhanced remote privacy checking

To cite this article: Ran Vijay Singh and L Agilandeeswari 2017 *IOP Conf. Ser.: Mater. Sci. Eng.* **263** 042006

IOP Conf. Series: Materials Science and Engineering **263** (2017) 042006 doi:10.1088/1757-899X/263/4/042006

Secure open cloud in data transmission using reference pattern and identity with enhanced remote privacy checking

Ran Vijay Singh and Agilandeeswari L

School of Information Technology and Engineering, VIT University, Vellore-632014, Tamil Nadu, India.

E-mail: mail2agi05@gmail.com

Abstract To handle the large amount of client's data in open cloud lots of security issues need to be address. Client's privacy should not be known to other group members without data owner's valid permission. Sometime clients are fended to have accessing with open cloud servers due to some restrictions. To overcome the security issues and these restrictions related to storing, data sharing in an inter domain network and privacy checking, we propose a model in this paper which is based on an identity based cryptography in data transmission and intermediate entity which have client's reference with identity that will take control handling of data transmission in an open cloud environment and an extended remote privacy checking technique which will work at admin side. On behalf of data owner's authority this proposed model will give best options to have secure cryptography in data transmission and remote privacy checking either as private or public or instructed .The hardness of Computational Diffie–Hellman assumption algorithm for key exchange makes this proposed model more secure than existing models which are being used for public cloud environment.

1. Introduction

Cloud computing is characterized as a sort of processing that depends on exchanging registered database as opposed to having nearest servers or any devices to concern with applications stored on them . The cloud environment administration is basically encountered with an expansive scope of inner/outer intruders, who might vengefully erase or degenerate clients' information [1]. Open cloud storage server is the place where anything can be stored and shared digitally in an inter domain network which is free of cost .But it creates issues due to data storage on a third party's standards which make risks for client's privacy that means clients may lose control over their data [2, 3].That means clients need reference about what data has to be transferred to cloud and how it will be managed. So, it is very important to secure real time based open cloud environment to let the processing has to be done by client's or data owner be robust and reliable. So client should have aware of what provisions are being used for backup, encryption and privacy checking .It is must to ensure the authorized person to view what is to be shared in an inter domain network. There is service that is provided in form of software delivery which gives the accessibility to software's and their processing via remote server. There is service that is based on platform framework which provides purchasing and controlling the software. Another one service is provided as purchasing of remote severs and software based on use or demand .Ensuring that our data is secured or not it is big concerns about security of information. It includes remotely privacy checking, client's authenticity, login access,

checking of any compromised data, security of key generation and sharing that is to be addressed in cloud computing environment [4 - 5].

Open cloud is also known as software as a service that means they provide the storage publically to clients. It is generally the internet. Private cloud is basically owned by companies in data centers for remote monitoring and automation. It is used by large scale companies. Hybrid cloud is used by companies as both public and private cloud .They uses it to maintain the control over private cloud and if any unwanted this happens they go for public cloud demand [6 - 7]. There should have best re-evaluating technique to know bandwidth requirements based on a continuous stream of frames in both directions. In this project which is based on attribute and reference pattern cryptography designed by computational Diffie-Hellman assumption algorithm and an additional enhanced remote privacy checking technique as extension. Computational Diffie-Hellman concept is used for security of cryptography system which is based on discrete logarithmic assumption. Let consider a cyclic group G of order q and there is given some groups G and their group components g, and the components g_a and g_b will calculate the value gab. It defines that (g, g_a, g_b) is chosen randomly for key generator g and randomly taken a ,bϵ{0,….,q-1} to calculate the result g_{ab}. CDH assumption based algorithm let us to calculate the DH shared secret key. This provides CDH problem more hardness using the algorithmic function F(g_{ab}) to obtain the result of gab needed by CDH ,in that term security of cryptography system is achieved at high. This proposed concept use Diffie-Hellman assumption algorithm for the all files that have been transmitted and proper splitting of frames. File Splitting will make easy for the administrator to maintain the records. Use of Diffie–Hellman computational assumption algorithm in key generation for clients make this proposed model used in this paper more secure than existing models which are being used in open cloud environment .This concept will provide more effectiveness and high data transmission rate and enhanced performance and secure storage and sharing of data.

2. Scope

This paper which is based on an identity based cryptography in data transmission and intermediate entity which have client's reference with identity that will take control handling of data transmission in an open cloud environment and an extended remote privacy checking technique which will work at admin side .On behalf of data owner's authority this proposed model will give best options to have secure cryptography in data transmission and remote privacy checking either as private or public or instructed .The hardness of Computational Diffie–Hellman assumption algorithm for key exchange makes this proposed model more secure than existing models which are being used for public cloud environment .This model will be more effective, secure, trusted and performance will also be enhanced.

3. Objective

In this paper, cryptography based on identity and reference pattern is designed from hardness of computational Diffie-Hellman assumption algorithm for key exchange and an additional enhanced remote privacy checking technique which provides better security for all files transmission in the open cloud with the hardness of techniques being used. Data will be shared into proper split frames and inter domain will be remained synchronized.

4. Existing System

In existing concepts file can be easily hacked during data transmission on open cloud environment when the server out of synchronization mainly due to improper streams of split frames and there is remained the problem for clients if they are restricted by open cloud server to have access control on

files for sharing and there was not exact proof of privacy checking techniques. The storage server could have unconsciously deleted the hosted data and sometime there was slow rate of storage.

5. Proposed Framework

In this proposed framework regarding to client that need to put in their information to be stored in an open cloud storage server before that client will have to give login credentials in user interface system if it is true then they shall proceed further if not then they will have to do signup first .During uploading of file key will be generated that will be used for encryption and one attribute from client's credentials will be added with file in open cloud. The data of file will be stored in cloud storage server in a proper splitting of frames .If any other user of that group member or network wants to download that file first of all they will have to get authentication from data owner as request of shared secret key to data owner and that specific attribute .After getting these details only receiver can go to download file where decryption process will be done. Use of computational Diffie-Hellman assumption algorithm make cryptography secure, robust and synchronized network of group members. Sometime clients are restricted to access to open cloud storage server directly due to some error then there is an Intermediate entity as reference of data owner which takes control of data owner to take care of processes. It will not let the data transmission rate be lower. This way data can be shared between inter domain network easily data will also be secured. Remote privacy checking technique will work as extension in open cloud server which will check data integrity and confidentiality remotely. It will work at admin side. So it makes the proposed solution framed in this paper very strong, secure, effective, and productive. It is shown in Figure 1

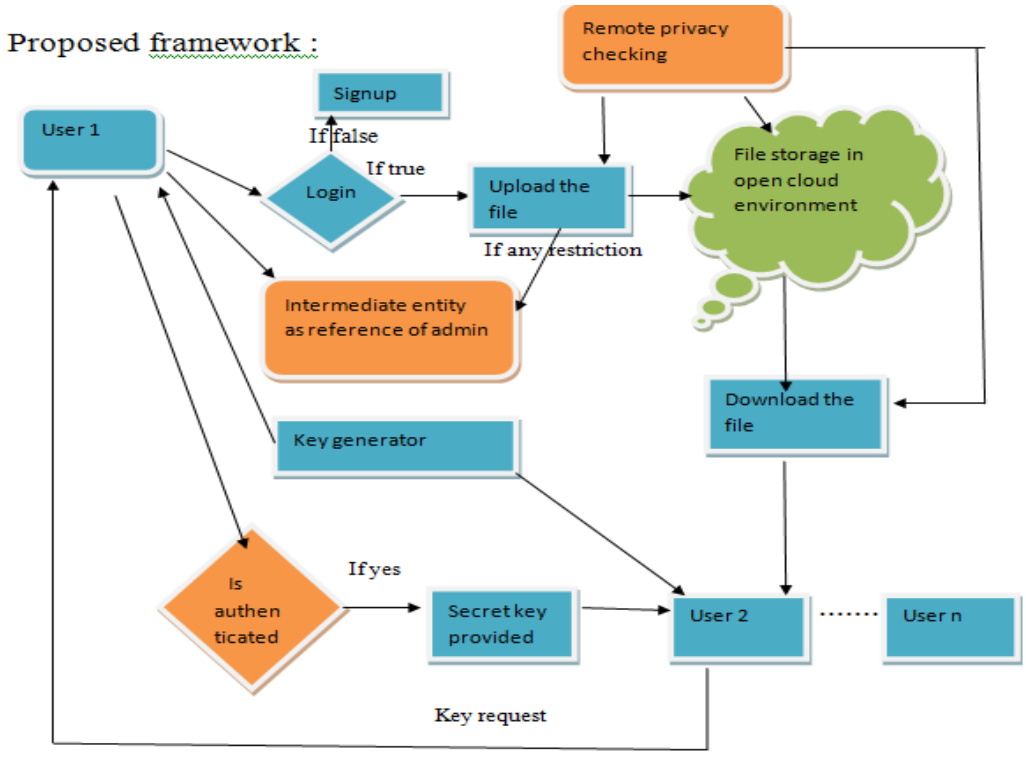

Figure 1. Proposed framework

6. Methodologies

In this paper we give the formal definition, structure model and security model. There are six models in this paper that makes concept unique and more secure than existing concepts. Here we describe about every stages with their figure and explanation. Methods, algorithms and diagrams are provided below with explanation.

6.1. Various stages of system

The proposed system involves various stages namely,

a. User interface design
b. Data upload
c. Key generate & file sharing
d. Key request to data owner
e. Data share in inter domain
f. Enhanced remote privacy checking

6.1.1. User Interface Design.

In this first stage of paper the significant role is regarding the user to redirect them from login page to data owner page as shown in Figure 2. This module also has made to provide the secrecy utility. There is registration page where client have to submit the login information like the username and the password and other required details. Thus, the function will verify whether the username and the password is matched or not with database at login page (validation of the username and the password). In order to entry if anyone has submitted the wrong username or the wrong password they can't be authorized to be go further from the login page to the user's very own page, an error message will be shown. That's why we are trying to assure that only authorized used only can access to Login page. This will equip a robust secrecy to this work. Here cloud based server will store the username and the password from local database and also watch on authenticity of client. This will provides an improvement in the security and debar from unauthorized data owner's entry at the server. In this paper, Java swing has been used to create the user interface. The function being used will verify the login that is, user's identity and accessing authentication.

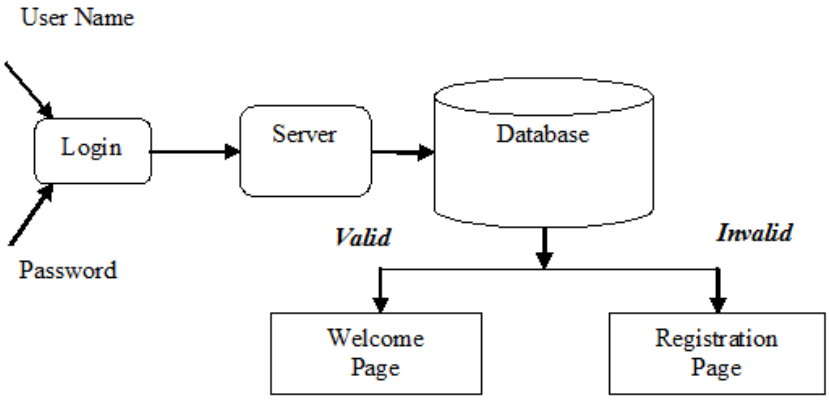

Figure 2. User Interface Design

6.1.2. Data upload

This module is used to help the user to uploading the files. At the time of login, if the user is a valid user means he is verified by server then only they will be allowed uploading their files.

6.1.3. Key generates and files sharing

This stage is used to help the group members to share the files and check their file is safe or not that provides protection (see Figure 3). Key Generation is the process for generating keys to our files. Key generation process is based hardness of Diffie-Hellman key exchange algorithm. That key will have to be a private for every group member while at the time of receiving.

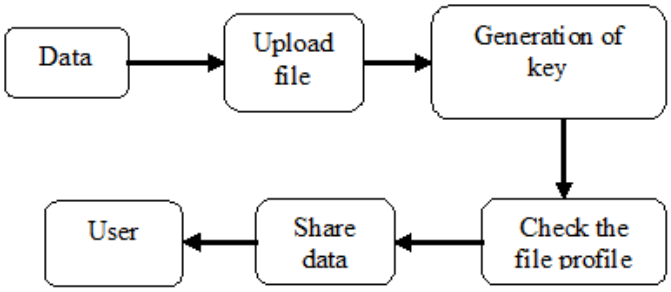

Figure 3. Key generates and files sharing

6.1.4. Key request to data owner

In this stage the file is only in view format so the file is sharable and download purpose can be done by only send request to the data owner, the data owner has to check the request and allow if user is an authorized person so data owner response and key provide to the user as shown in Figure 4.

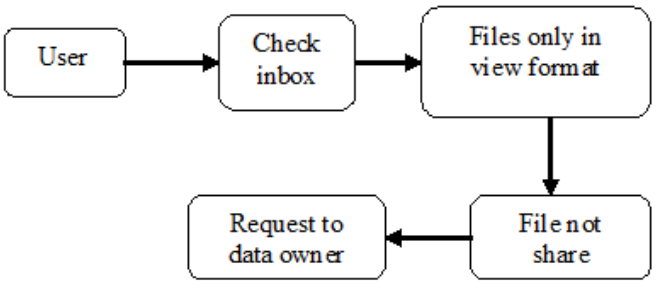

Figure 4. Key request to data owner

6.1.5. Data sharing in inter domain

In this stage the key is provided by the data owner to the user and obtains the ownership for current data. So user can share the file with group members and also can download the file as in Figure 5.

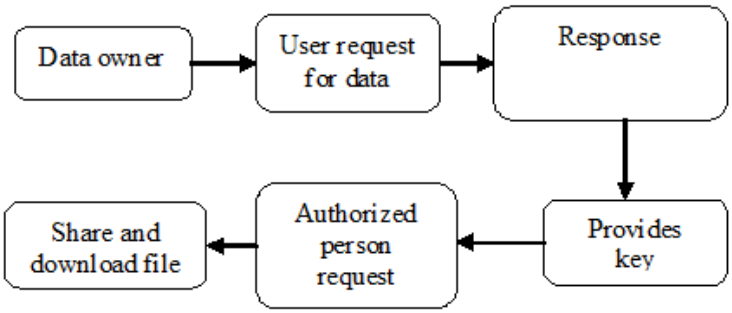

Figure 5. Data sharing in inter domain

6.1.6. Enhanced remote privacy checking

In this stage privacy checking technique is used in form of extension which will be under control of admin. This module is used to check whether user who wants to access request is valid or not and data that is being shared are secured or not. It is responsible for to make integrity and confidentiality of data be robust.

7. Results and Discussions

In this paper as we can see the technologies, methods, algorithms used in our proposed concept makes real time environment based open cloud server robust, highly secure, and reliable. Security models used in authentication process, file storage in cloud server, key generation and sharing them to users, uploading and downloading of files, request list sent to owner are very unique. Concept of Reference pattern design used in this model for users to save the time and easy storage of data on server making inter domain network synchronized. Output obtained in order to implementation are provided below with explanation,

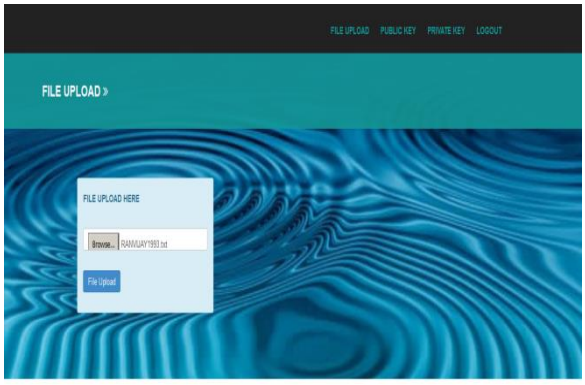

Figure 6. File Upload

Figure 6 shows file uploading section. Here we can select any pdf file to upload. Now, file has been uploaded and if any user wants to download the file that is already had been uploaded by other persons of that group then they will have to send the request to Admin for access of data as in Figure 7.

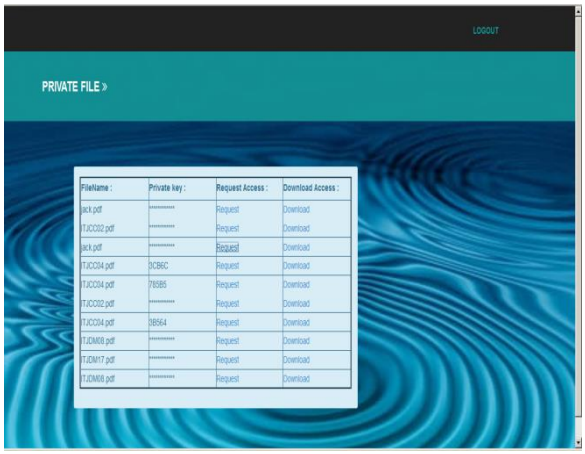

Figure 7. Request to Admin

Admin will check the updated list of requests sent by user and then Admin will allow the user by sending a secret key after authentication process done as shown in Figure 8. For downloading the file as in Figure 9, user will have to submit the same secret key that was sent by admin to download the file.

Figure 8. Request Acceptance by Admin

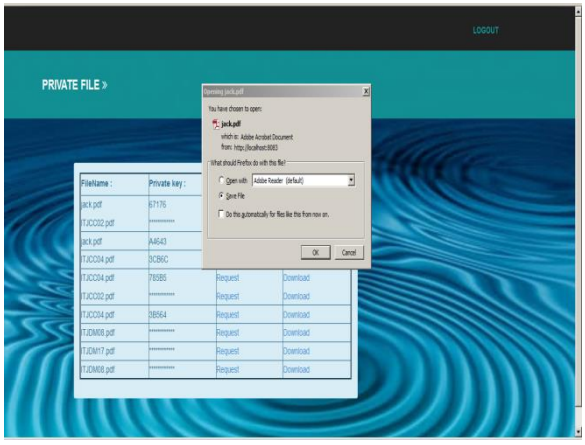

Figure 9. File Download

Key generation process has been done by using computational Diffie-Hellman key exchange assumption algorithm to make security robust and data also been confidential. If any interference is happened during uploading or downloading of file or storage speed is very slow then Reference pattern design on behalf of data owner will take control later to complete the process. It will improve the productivity of real time based cloud storage. Remote privacy checking will be done at admin server side which will check authenticity of user and confidentiality and integrity of data.

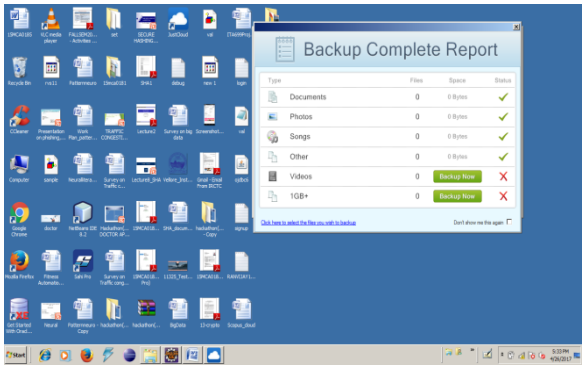

Figure 10. Cloud Storage Backup report

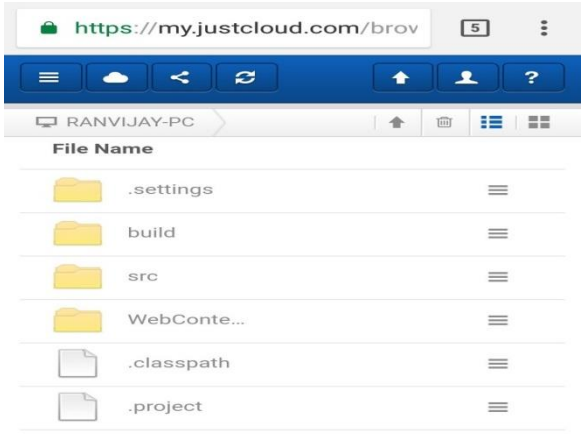

Figure 11. Cloud Storage Folder

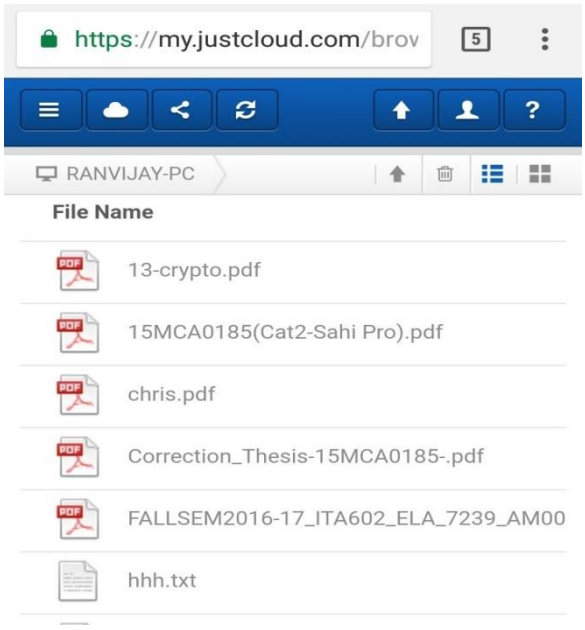

Figure 12. File download from cloud storage

Here as far as real time base cloud environment is concerned. We have used Just Cloud tool that provides open cloud storage. We have connected our local database server to this Open cloud tool. Files that are being uploaded or downloaded will be checked remotely by admin that will provide confidentiality. Techniques, algorithms used in this paper make file transfer among inter domain group members very secure and storage speed at high rate. It increases the productivity of file exchange in open cloud as shown in Figure 10, 11 and 12.

8. Future Enhancement

In this paper the concepts and methods that have been used can be enhanced on big level in IT industries. Modules used in this proposed concept are very unique and robust so it can be used in future prospect of cloud computing environment. It can be enhanced further according to demand of future technology for open cloud security.

9. Conclusion

This paper is mainly based on transfer of data and their security how will be secured in open cloud real time environment. Here we have provided the solution for this problem. Ideas which have been used in this paper make it a secure and robust technique to be used in open cloud environment. These techniques make the key generation and sharing, data uploading and downloading, remote privacy checking based extension very confidential and secured .It makes techniques used in this paper better than existing techniques.

References

[1] Ren Y, Wang J, Shen J, Han J and Lee S 2015 Mutual verifiable provable data auditing in public cloud storage *J. Internet Tech.* **16** 317-23
[2] Ateniese G, Di Pietro R, Mancini L V and Tsudik G. 2008 Scalable and efficient provable data

possession *ACM Proceedings of the 4th Int. Conf. on Security and privacy in communication netowrks* 9
[3] Wang H 2013 Proxy provable data possession in public clouds *IEEE Trans. Ser. Computing*. **6** 551-59
[4] Anand D, Khemchandani V and Sharma R K 2013 Identity-based cryptography techniques and applications (a review) *IEEE 5th Int. Conf. On Computational Intelligence and Communication Networks (CICN)* 343-48
[5] Ren Y, Shen J, Wang J and Fang L 2014 Security Analysis of Delegable and Proxy Provable Data Possession in Public Cloud Storage *IEEE Tenth Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)* 795-98
[6] George R S and Sabitha S. 2013 Data anonymization and integrity checking in cloud computing IEEE *Fourth Int. Conf. On Computing, Communications and Networking Technologies (ICCCNT)*,1-5
[7] Esiner E, Küpçü A and Özkasap Ö 2014 Analysis and optimization on FlexDPDP: A practical solution for dynamic provable data possession *Int. Conf. on Intelligent Cloud Computing* 65-83