NCICIT 2013: 1st National Conference on Intelligent Computing and Information Technology, November 21, CUET, Chittagong-4349, Bangladesh

User-Authentication Approach for Data Security Between Smartphone and Cloud

Md. Al-Hasan[1], Mohammad Obaidur Rahman[1], Md. Ashraf Uddin[1]
[1]Department of Computer Science & Engineering, Chittagong University of Engineering & Technology, Chittagong - 4349, Bangladesh
Email: hasan07cse@gmail.com; obaidur_91@yahoo.com; rash.cuet@yahoo.com

***Abstract*—Cloud computing architecture provides a proper management to share distributed resources and services throughout the world via computer network. This architecture offers three main features, e.g. SaaS, PaaS and IaaS. And today's Smartphones are more compatible with this architecture, especially with IaaS because of its small storage capacity. Smartphones have become almost computer and these can be viewed as a miniature of personal computer. Since cloud computing share distributed data via network in the open environment so, there may occur security problems. To address this problem, this paper has proposed a new data security approach for Smartphone in cloud computing architecture, which ensures secured communication system and hiding information from others. Security level is maintained using the Global Positioning System (GPS) and network provider which ensures strong user-authentication to secure our cloud.**

Keywords: Cloud Computing; Smartphone; Data Security; RSA; El Gamal; DES; AES.

I. INTRODUCTION

In the recent time, cloud computing has become a most frequently talked and attractive phenomenon among the people all over the world. Though this is the newly introduced term in IT industries, but the fact inside it is more common and primitive technology of computer network. Today cloud computing has won people's heart and become appealing enough to collect billion of customers for itself. And the increasing number customers have become a major threat for cloud computing environment which results in security problem of customer's valuable data.

In cloud environment, resources are shared among all of the servers, but users don't know the fact that how their data are stored in the server. Because there is a lots of data of each user's stored in the server and user don't know which data is located in which database server and how [1]. That's why it is very easy for an intruder to access, misuse and damage the original form of data. For this it is also very much essential for the cloud to be secure through proper resource management [2]. Today, there is a variety of security models and algorithms are applied in the field of cloud computing. But, these become failed to meet all aspects security threats [3]. In E-commerce and online business, we need to involve high capacity security models in cloud computing. File encryption system based on AES is used in some thesis work [4]. DES based file encryption system is also worked out [5]. But their given models keep both the key and encrypted file in the same database server. Some thesis works have tried to recover this problem [6]. All of their approaches are suitable for some respective aspects but, don't cover all criteria to make a system secured.

Till now, we are talking about the data-security in the cloud computing architecture. But, what will be our secured approach if the user terminal is Smartphone [7]. Today's Smartphones have spurred a renaissance in mobile computing and can be viewed as a miniature of personal computer having all capabilities of it. As Smartphone is of limited storage and there is a fear of losing the phone, cloud can be a greater solution to this problem. But, there should be a well-defined approach for user-authentication of Smartphone and data-security in the cloud. This thesis work has proposed a new approach to data-security in Smartphone through stronger user-authentication.

II. METHOD

This thesis-work ensures data-security using two encryption algorithms:

- Public Key Encryption Algorithm
- Private Key Encryption Algorithm.

Here, in Fig. 1 public key encryption algorithm is used for prevent hacking of data in the communication line between the Smartphone and main server. That mean, it ensures secured channel for passing our data. And private key encryption algorithm is used for maintaining proper authorization of data and store encrypted data in the server so that the data will be useless if anyhow intruder get access to the database server. It should be mentioned that the decryption key of data will not be in the database server.

Stronger user-authentication is maintained using the decryption key of respective file and current location of the Smartphone using GPS (Global Positioning System).

Our proposed working model of cloud computing is depicted in Fig. 1. Here, we have made simulation to

get appropriate algorithm using this cloud model and also deploy this model with more security with simulated data.

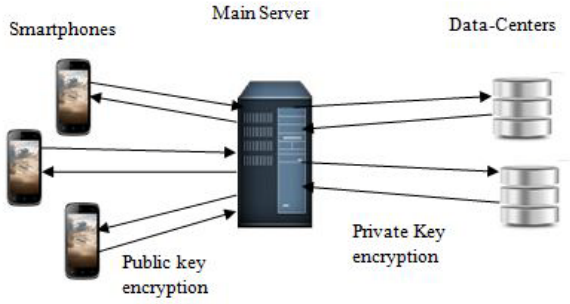

Figure 1. The Proposed Cloud Computing Model

In Fig. 1, we can see that the Smartphone user needs to contact with the main server to communicate with databases or datacenter. It takes files from the mobile users, stores these files in different databases, which are connected with it and retrieve files from the databases to specific users whenever needed. In our proposed model, user data is encrypted using public key cryptographic algorithm. That means user-data is encrypted in the Smartphone with the public key of the main server. Then server will decrypt the data with its private key. This public key cryptography ensures the security of data between the user and the main server. Now, come to the private key cryptographic algorithm which uses the same key for encryption and decryption. In our model this algorithm is used to store data in encrypted form in the database and send the decryption key to the Smartphone user's mail-box so that the data will be useless for the unauthorized persons. As a result, we can ensure a stronger user-authentication while downloading the data because to download data we need the decryption key of respective data. And decryption key is stored only in the authorized person's mail-box. So, even getting access to users cloud intruder can't get the meaningful data. There are many private key and public key cryptographic algorithms. Now, the problem is that which private key algorithm and public key algorithm we should use for our proposed model. In the next part we have made a simulation to get best fitted algorithm for our proposed approach to provide secured cloud environment.

III. SIMULATION TO GET SUITABLE ALGORITHMS

Smartphone, a little device with the promise of doing various computational tasks as like as personal computer is the terminal device for using the cloud computing environment. There is a major concern for computing devices that is power. Proper and efficient computing can ensure proper power management [8]. And as a small device with little battery power we should select such an algorithm which would not make our small computing device busy and consume a relatively small amount of time for doing the encryption.

A. Simulation Environment

- Processor Core 2 duo 2.8 GHz
- RAM 2GB
- Windows 7
- Android 4.0.4
- Java-script, PHP, MySQL Server

B. Simulation of Public Key Algorithms

There are many public key algorithms in cryptographic world. We select popular two from these which give better security and flexibility. These are:

- RSA public key algorithm
- El Gamal public key algorithm

RSA requires less energy for generation of keys, encryption and decryption of the data [9]. Vijayalakshmi shows in her paper work [10] that energy consumption in El Gamal is greater than in RSA algorithm for the same task.We select one smaller exponent (e) or encryption key in the RSA encryption. But El Gamal requires two exponentiations for encryption [11]. Fig. 2 shows RSA encryption requires less time than El Gamal but, Fig. 3 show the opposite. The file is encrypted on the mobile and decrypted on server. So, our goal is to minimize the encryption time whatever the total cryptographic time as depicted in Fig. 4. We get some experimental data (see Table 1) from our simulation on RSA and El Gamal public key algorithm.

Table 1. File Encryption & Decryption Time in RSA & El Gamal

File Size (KB)	RSA			El Gamal		
	Encry-ption Time (sec)	*Decry-ption Time (sec)*	*Total Time (sec)*	*Encry-ption Time (sec)*	*Decry-ption Time (sec)*	*Total Time (sec)*
1	0.07	0.19	0.26	0.13	0.11	0.24
2	0.13	0.38	0.51	0.27	0.21	0.48
3	0.20	0.58	0.78	0.40	0.33	0.73
4	0.27	0.78	1.05	0.52	0.44	0.96
5	0.34	0.97	1.31	0.66	0.56	1.22
6	0.40	1.15	1.55	0.79	0.67	1.46
7	0.47	1.35	1.82	0.93	0.78	1.71
8	0.54	1.54	2.08	1.05	0.88	1.93

C. Simulation of Private Key Algorithms

Among the various private key algorithm, DES and AES is main which apply more secure technique to make the system save. Both the encryption and decryption is occurred in server side. So, there is no need to separately consider the encryption and decryption time. Because, our prime concern is that Smartphone has to perform upload and download in a

shorter cryptographic time. For this total time required to encrypt and decrypt the file is considered. Our simulated data in lab shows the following result (see Table 2) regarding DES and AES.

Table 2. Total Cryptographic Time (second) in DES and AES

File Size (KB)	DES Cryptographic Time (sec)	AES Cryptographic Time (sec)
1	0.03	0.05
2	0.06	0.09
3	0.08	0.14
4	0.11	0.18
5	0.13	0.23
6	0.16	0.28
7	0.19	0.33
8	0.21	0.38

In our proposed model, we are giving priority on the capability of the small device, Smartphone maintaining a standard security level. We compare execution time (encryption and decryption) of DES [12] with AES [13] depicted in Fig 5. We are not considering triple DES (3DES) here, because it has high execution time than DES and we already know that.

D. *Graphical Comparison*

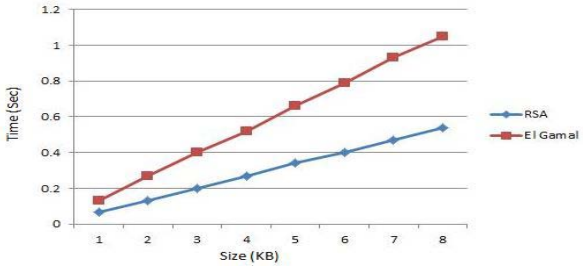

Figure 2. Encryption Time of RSA Versus El Gamal

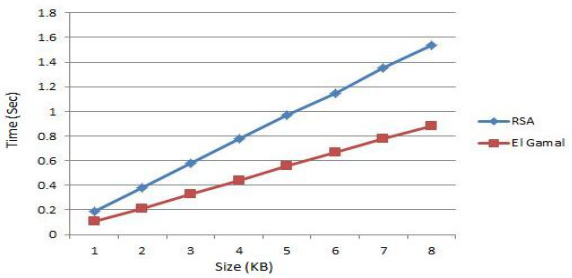

Figure 3. Decryption Time of RSA Versus El Gamal

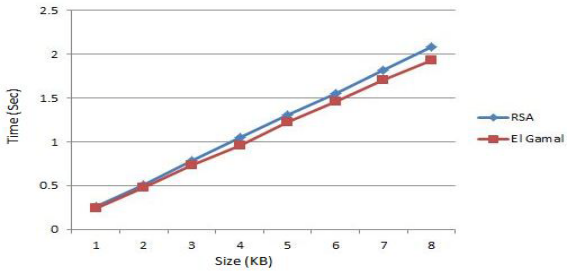

Figure 4. Total Cryptographic Time of RSA Versus El Gamal

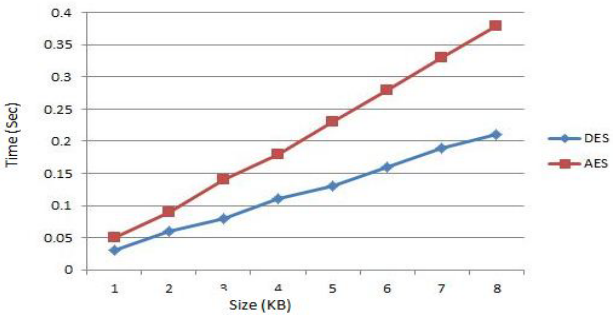

Figure 5. Total Cryptographic Time of DES Versus AES

IV. DEPLOYMENT OF THE PROPOSED MODEL

After making a proper simulation for our proposed model, we think that RSA and DES cryptographic algorithm is best suited for Smartphone to access the cloud. We have select RSA for its less encryption time (Fig. 2) as encryption occurs in Smartphone and our aim is to decrease computational time in Smartphone.

A. *File uploading to cloud*

In Fig. 6 RSA public key algorithm encrypt user's file in the mobile device with the public key (k1-) of the main server. And main server will decrypt this file with its private key (k1+) and encrypt the file again with DES private key algorithm using symmetric key, k2- and send the decryption key (k2+) to the user's mail-box. So, only authenticated user can get useful file from the database.

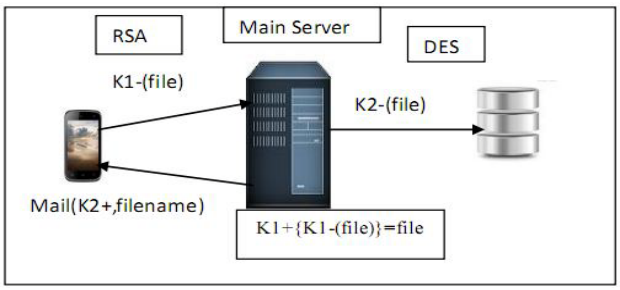

Figure 6. File Uploading to Cloud

B. *File Downloading from Cloud*

Fig. 7 describes the file downloading procedure. To download the files users have to login with their mail-id. One user may have many files in the cloud. So, users have to provide their corresponding file-name and DES decryption key (k2+) which was sent to their mail-box.

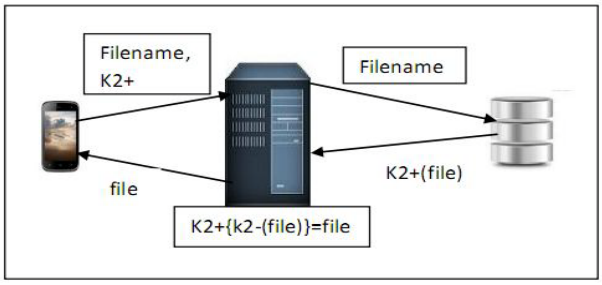

Figure 7. File Downloading from Cloud

C. *Ensuring Stronger User-Authentication to Secure User-data*

And finally we have tried to meet the cloud using mode of all users and provide them a more flexible way to get security at different level. Smartphone is the most personal device and users of it want Smartphone to be smarter reducing their own smartness or awareness. Users keep them always logged in the cloud in their Smartphone device to avoid several login. But, what will be happen to their cloud if the phone is lost or stolen intentionally to get access to personal data.

This is final step of deployment of our proposed model and this will provide greater flexibility to access a secure cloud from user's Smartphone offering different security mode. Here, we define three modes as the following:

1) Mode-1(Normal mode): In this mode we assume user is more smart and aware enough and logout each time of accessing cloud. So, he/she will follow the normal data-security model as described in file uploading and downloading section.

2) Mode-2(Secured Mode): This mode provides a high level security to the users. Here, a different database table (see Table 3) is maintained to ensure security.

Table 3. Database Table for Security Question

user_id (mail-id)	File-name	Security question	Answer (ans)
ab@yahoo.com	ac.txt otripto.txt …… …….	MD5(My first day at school?)	MD5(anS)
……	…… ……	……	……..

The above table is maintained by the authorized user. There may be a situation that user has lost his phone and all accounts (cloud account and e-mail account) browser are logged in as he prefers to do it. Now, it is very easy for intruder to get access to the cloud account as the key containing mail account and cloud account both are open to him. Then what will happen to the user's valuable data. To answer this question we propose this secure mode. Users can set more anonymous question and answer in a database table (see Table 3) to restrict intruder to get data. However, intruder will not get the actual answer or can't guess any answer from question if he/she gets access to database because; MD5 Message-Digest algorithm [14] is applied here. So, this secured mode restrict intruder with a security question.

3) Mode-3(Advance mode): If the user is in the regular location (location will trace through GPS of Smartphone and network provider) then use normal mode else use secure mode. Each of us has some particular working locations from where we access our cloud. We define these locations as regular location. So, our proposed model provides a strong user-authentication and by this way which indirectly maintain our data security.

V. CONCLUSION

In this thesis paper, we have worked to get a suitable cloud computing security architecture for Smartphone. Smartphone is a mobile and small device. So, the general traditional security approaches will not fit to Smartphone-cloud architecture. Considering its computing power and battery power we proposed RSA and DES algorithm in this architecture. And in final implementation of our proposed model we have tried to make a strong user-authentication considering its mobility. Ensuring the stronger user-authentication we ensure the data-security between Smartphone and cloud.

REFERENCES

[1] M. A. Vouk, "Cloud Computing – Issues, Research and Implementations", *Journal of Computing and Information Technology - CIT 16*, vol. 4, pp. 235–246, 2008.

[2] Y. Hu, J. Wong, G. Iszlai, M. Litoiu, "Resource Provisioning for Cloud Computing", *IBM Canada Ltd.*, 2009.

[3] N. G. Mollet, "Cloud Computing Security", Thesis Paper, April 11, 2011.

[4] Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman, "FADE: Secure Overlay Cloud Storage with File Assured Deletion", 2010.

[5] N. Jain and G. Kaur, "Implementing DES Algorithm in Cloud for Data Security", *VSRD-IJCSIT*, vol. 2 (4), pp. 316-321, 2012.

[6] T. S. Kar, M. A. P. Mahmud, "A Newer Secure Communication, File Encryption and User Identification based Cloud Security Architecture" *International Journal of Computer Applications (0975 – 8887)*, vol. 52– No.4, August 2012.

[7] (2013, Aug.) The Wichita education website. [Online]. Available: http://webs.wichita.edu/depttools/depttoolsmemberfiles/wines

/4A_Tandel_Venkitachalam_Cloud-Computing_Smartphones.pdf

[8] G. Dhiman and T. Š. Rosing, "System-Level Power Management Using Online Learning", *IEEE Transactions On Computer-Aided Design Of Integrated Circuits And Systems*, vol. 28, no.5, May 2009.

[9] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM*, vol. 21, Feb 1978.

[10] Kayalvizhi.R, Vijayalakshmi.M, Vaidehi.V, "Energy Analysis of RSA and ELGAMAL Algorithms for wireless Sensor Networks", Proceedings of the 8th WSEAS International Conference on Applied Electronics, Wireless and Opticalal communication, 2012.

[11] T. El Gamal, "A public key cryptosystem and a signature scheme based discrete logarithms", *HP labs*, 1985.

[12] R. G. Kammer, W. M. Daley, "Data Encryption Standard (DES)", *Federal Information Processing Standards Publication*, FIPS PUB 46-3, 1999.

[13] J. Daemen, V. Rijmen, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", *Federal Information Processing Standards Publication 197*, November 26, 2001.

[14] Ronald Rivest, "MD5 Message-Digest Algorithm", *rfc 1321*, April 1992.