New Homomorphic Platform for Authentication and Downloading Data in MCC

Karim ZKIK, Maha TEBAA, Said EL HAJJI

***Abstract*— In order to promote their products and interact easily with customers, companies use services of mobile Cloud computing increasingly. This new concept offers the possibility for mobile users to acquire any kind of products, and benefit from many services just by using their mobile device. The use of these services requires in many cases sharing highly sensitive information, as in the case of online payment services where user has to enter his credit card code and other sensitive information. So, the problems related to security and privacy are the first obstacles to the deployment and expansion of these services use. We propose a security structure that allows mobile users to download data from a distant cloud server, and so ensure the confidentiality and integrity of data and user privacy. This structure is composed of an authentication mechanism that uses the homomorphic encryption, and a download mechanism that ensures the privacy and security of data. It is proposed thereafter an evaluation and implementation of our platform, which demonstrates that our structure guarantees the authenticity and privacy of mobile users, and offers a high level of data security.**

***Index Terms*—Mobile Cloud Computing, security, homomorphic encryption, secure download**

I. Introduction

Mobile Cloud Computing (MCC) [1] is concept, where applications and mobile data are downloaded, stored and hosted using cloud computing technology [2-5]. The MCC storage services have become increasingly popular during the last years and more adopted by mobile users (19% of mobile users in 2014) [6], but requiring more capacity and processing power.

Security threats and risks related to security and user privacy are the main obstacles to adaptability and rapid expansion of storage services use in the MCC [7-10], and more than 74% of IT Executives are not interested by the implementation of Cloud computing services because all this security's problems [11-12]. So, using the Mobile Cloud computing storage services is still very limited, particularly for storing and downloading sensitive personal data, because companies and users of Cloud computing services are afraid of losing their data or that attackers seize it.

Kamara et al. [13] have defined one of the first security architectures using the cryptographic function for storing data in the mobile cloud. Its structure ensures the confidentiality of shared data between mobile users and cloud server. Hsueh et al. [14] proposed a scheme to ensure security and integrity of mobile users files stored in the cloud, and introduced an authentication mechanism to authenticate the owner of the file downloaded from the cloud server. This scheme relies on the services of a certification authority that ensures integrity by using traditional hash signature. Zhiwei et al. [15] defines a new homomorphic signature for identity management in mobile cloud computing to compute a homomorphic signature on all users sensitive personal data in MCC.

Our security system is primarily dedicated to companies and organizations that use the Cloud Computing services to storage of their sensitive data and their customers personal data in order to have more storage space, to obtain more resources, and to increase their services quality. So, the goal of our platform is to offer to customers, especially mobile users, the ability to access and download their data using Mobile cloud computing services safely, while ensuring their integrity and privacy. So, we will construct a new secured homomorphic platform for a secure downloading and authentication in the MCC. This platform will firstly allow mobile users to authenticate to a central server safely, and to ensure their data integrity by using a homomorphic signature based on the algorithm proposed by Zhiwei et al. [15], and then download and consult safely their personal data stored in the corresponding private cloud server.

We will also present an application in which we will make the implementation of our security framework. We will choose for our security scheme a scenario that focuses on bank data. This scenario will allow mobile users to authenticate and download their sensitive bank data stored in the cloud server.

I. Problematic and Architecture Description

A. Problematic

The goal of our work is to develop an architecture that ensures connection between mobile users and the cloud server in such a way that mobile users can download and interpret their personal data safely.

To develop our security structure we need first to respond to security issues:

Manuscript received February 24, 2015; revised March 04, 2015.

K. ZKIK Author is with Laboratory of Mathematics, Computing and Applications, Faculty of Sciences, University of Mohammed V-Rabat, Rabat, Morocco (corresponding author to provide phone: +212-668-514-985; e-mail: Karim.zkik@gmail.com).

M. TEBAA Author is with Laboratory of Mathematics, Computing and Applications, Faculty of Sciences, University of Mohammed V-Rabat, Rabat, Morocco (e-mail: maha.tebaa@gmail.com).

S. EL HAJJI Author is with Laboratory of Mathematics, Computing and Applications, Faculty of Sciences, University of Mohammed V-Rabat, Rabat, Morocco (e-mail: elhajji@fsr.ac.ma).

ISBN: 978-988-19253-4-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

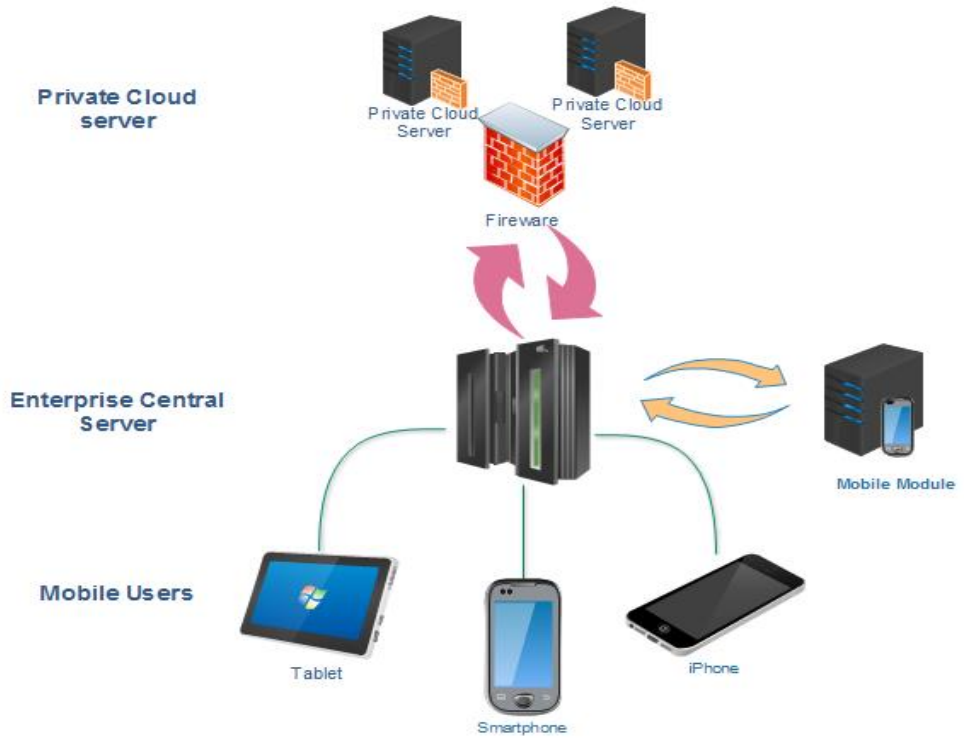

Fig. 1. Basic scheme of our proposed model

- The connection between mobile user and server must be secure and must be able to ensure his data integrity and safety.
- Data stored in cloud server is encrypted with the public key PK_{SC} of local server following a homomorphic encryption scheme [16]. Mobile user will be unable to interpret data sent from cloud server.

To avoid these problems, we will develop an authentication system that will allow users to authenticate securely in local server, and then we will develop a downloading system that will allow them to download safely and interpret their sensitive data from the private cloud computing server.

A. *Proposed model*

We will propose a new framework which allows mobile users to access their data stored in the private cloud computing server.

Our basic scheme as shown in Fig. 1 contains four main entities: The mobile device (DM), the central server (SC), a mobile unit (MU), and the private cloud computing server (PCS). The mobile device is responsible for downloading data from the cloud server. The local server authenticates users and ensures communication between the mobile device and the cloud server. The cloud server sends the asked data to the local server, which redirects it to the mobile device.

Our security scheme is divided into two parts:

- The first part concerns mobile users authentication.
- The second part concerns data downloading from our private cloud computing server.

It is assumed that our central server can store and download data safely from the private cloud server; data is encrypted and decrypted using the secret key SK_{CS} and the public key SK_{SC} of our central server.

II. Authentication Scheme

We will present in this part a mechanism to authenticate the owners of files downloaded in the private cloud computing server.

The authentication scheme ensures the authenticity of the mobile users and the integrity of requests and communications between the mobile and the server.

The mobile device forges a homomorphic signature to ensure the integrity of requests and data on the basis of the algorithm Z. Wang and al. [15], and then it sends an authentication request to the central server. The central server asks its responsible mobile unit to check validity of authentication requests issued by mobile user.

A. *Homomorphic Signature Scheme*

Some attacks aim to forge valid signatures in order to impersonate mobile users, and recover their sensitive data stored in the cloud [17-18]. The goal of our scheme is to construct homomorphic signatures [19] impossible to forge by attackers.

Every mobile user should have an ID for authentication, account number (AN) to access personal data stored in the cloud server and mobile device number (DN). Mobile users create their own signatures from their personal data (PDM) as: PDM = (AN, ID, DN)

Mobile device generates a public key PK_{DM}, and a private key SK_{DM}. We assume that the validity time t, the public key PK_{DM}, and the user ID are properly distributed among mobile devices, the central server and the mobile unit.

ISBN: 978-988-19253-4-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

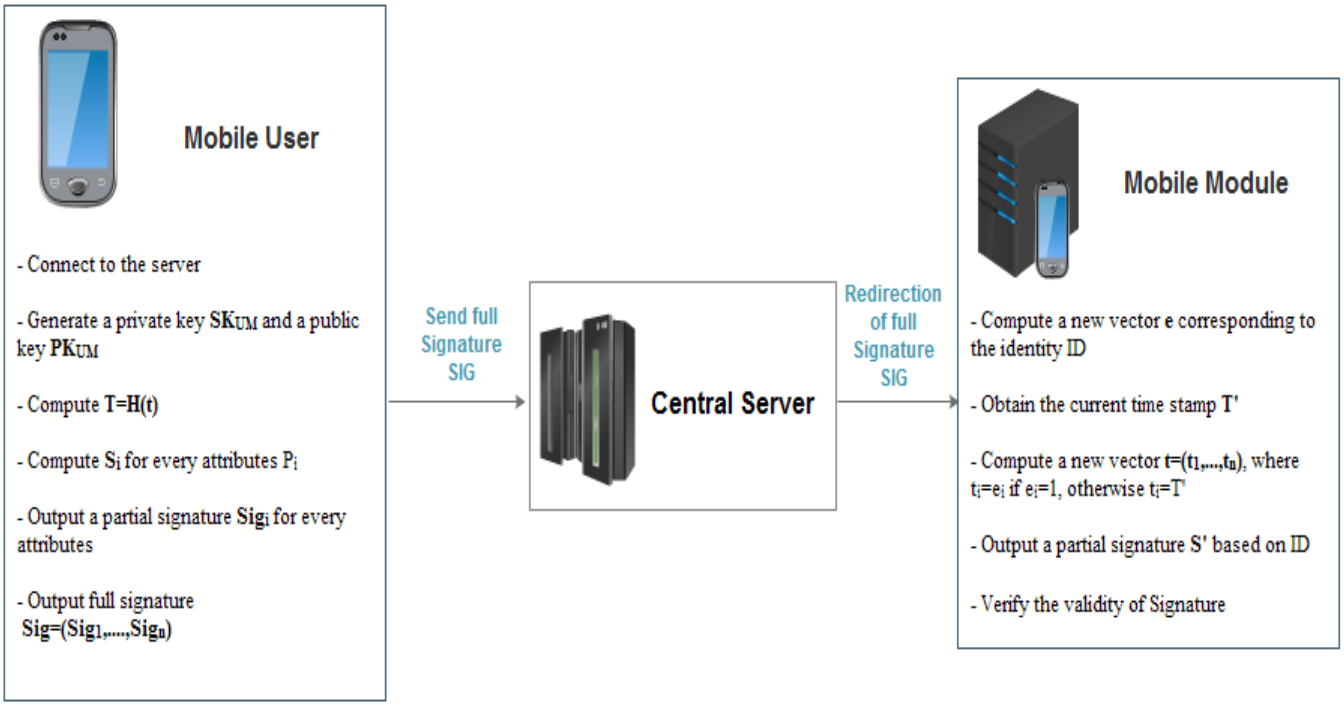

Fig. 2. Homomorphic Signature Scheme

For forging our signatures homomorphic, we proceed as shows in Fig. 2:

1- Mobile connect to the server using his login and his password
2- Mobile generate a private key SK_{UM} and a public key PK_{UM}
3- We will choose t as a period of validity and we will compute T=H(t), as H is a hash function
4- We choose a random elements $v=\{v_1,...,v_n\}$, $r=\{r_1,...,r_n\}$ and u.
5- We divide every elements of PDM into several part Pi as P={P1,……..,Pn), and we compute for every parts:

$$S_i=((r_i)^{P_i}\times u^{v_i})^{1/T}(\text{mod } N) \quad (1)$$

6- The full signature is :

$$Sig=(Sig_1,...,Sig_n) \text{ as } Sig_i=(S_i,v_i,T) \quad (2)$$

7- The mobile device send the full signature to the central server, and our central server redirect the full signature to his mobile unite
8- The mobile unite Compute a new vector $e=(e_1,...,e_n)$ corresponding to an identity ID of the user
9- Compute a new vector N:

$$N=(N_1,...,N_n), \text{ where } N_i=e_i \text{ if } e_i=1, \text{ otherwise } N_i=T'. \quad (3)$$

T' *is the current time stamp*

10- Output a partial signature on ID S':

$$S_i^{'}=\prod_{i=1}^{n}S_i^{N_i} \quad (4)$$

11- Compute x

$$x=\prod_{i=1}^{n}r_i^{P_i}\times u^{v'} \text{ as } v'=\sum_{i=1}^{n}N_i\times v_i \quad (5)$$

12- verify the Signature :

$$\text{if } Sig^T=x(\text{mod } N) \text{ output 1, otherwise output 0.} \quad (6)$$

A. *Mechanism of Authentication*

Each mobile user must authenticate in the mobile unit to receive a password (PWD), which will allow him to access and view his personal data in the cloud server. To do so, we will develop a secure authentication scheme. The proposed secure scheme works in four steps as shown in the Fig. 3.

It is assumed that the user is already connected to the central server. Public key generated by mobile unit PK_{UM}, and the user's identity (ID) are properly distributed among the mobile devices, the central server, and the mobile unit.

The algorithm of authentication is as follows:

1- First each user sends an authentication request to the central server, this application is defined as:

$$MD\mapsto CS: E_{PK_{UM}}(NC, ID, DN), Sig \quad (7)$$

2- Then the central server redirects the request to his mobile unit

ISBN: 978-988-19253-4-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

$$CS \mapsto UM : E_{PK_{UM}}(NC, ID, DN), Sig \quad (8)$$

3- Mobil Unit checks the validity of the request, and the authenticity of the homomorphic signature, before generate a password (PWD) which will allow the mobile user to access to the cloud server. The mobile unit sends the PWD to the central server.

$$UM \mapsto CS : E_{PK_{MD}}(NC, ID, DN, E_{PK_{MD}}(PWD)) \quad (9)$$

4- Finally the central server redirects the PWD to the Mobile User

$$CS \mapsto MD : E_{PK_{MD}}(NC, ID, DN, E_{PK_{MD}}(PWD)) \quad (10)$$

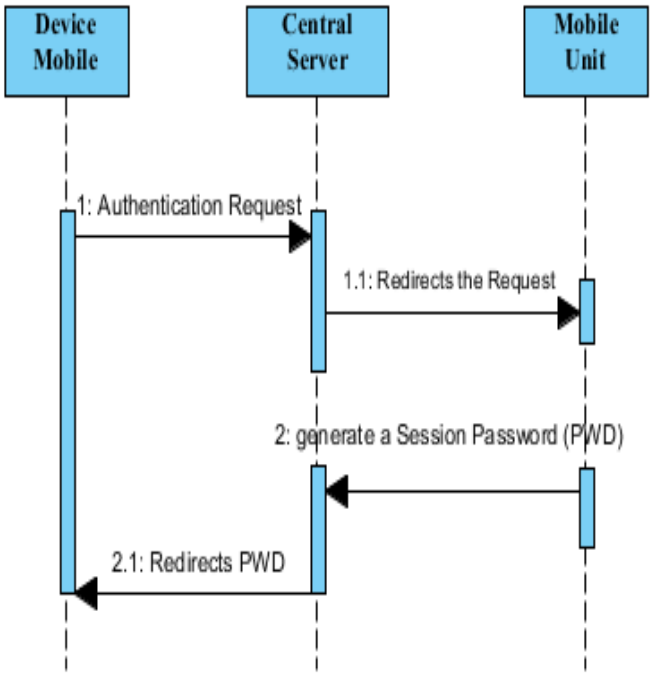

Fig. 3. Authentication Scheme

Our authentication scheme allows users to connect securely to our central server and retrieve a session key to connect later the Cloud server. Our scheme uses a homomorphic signature to ensure the integrity, queries between different entities are encrypted which ensures confidentiality and for each connection, the user needs to retrieve a new session key which allows to secure user accounts and prevent replays attacks.

III. Downloading Scheme

After authentication, we will propose in this section an architecture that allows mobile users to view and download their sensitive data safely.

In our model we assume the data stored in the private cloud server are encrypted with the public key PK_{SC} of our central server.

Our basic scheme as shows in Fig. 4, contains three main entities: The mobile device (DM), the central server (SC), and the private cloud computing server (PCS).

The downloading algorithm is as follows:

1- For downloading his personal data from the private cloud server The mobile user sends a request to the central server.

$$MD \mapsto SC : E_{PK_{CS}}(NC, ID, PWD, Ri), Sig \quad (11)$$

$R = (R_1, ..., R_n)$ *such that each* R_i *is a type of request*

2- The central server verify the validity of the signature and then redirects the request to the private cloud server.

$$SC \mapsto PCS : E_{PK_{PCS}}(NC, ID, PWD, Ri), Sig \quad (12)$$

3- Cloud server consults his database before sending the encrypted data to our central server.

$$PCS \rightarrow SC : E_{PK_{SC}}(DATA), Sig \quad (13)$$

4- The server decrypts the data with his secret key SK_{SC}, and re-encrypted with the public key of the mobile user PK_{MD}, and then redirects data to the mobile device.

$$PCS \rightarrow SC : E_{PK_{MD}}(DATA), Sig \quad (14)$$

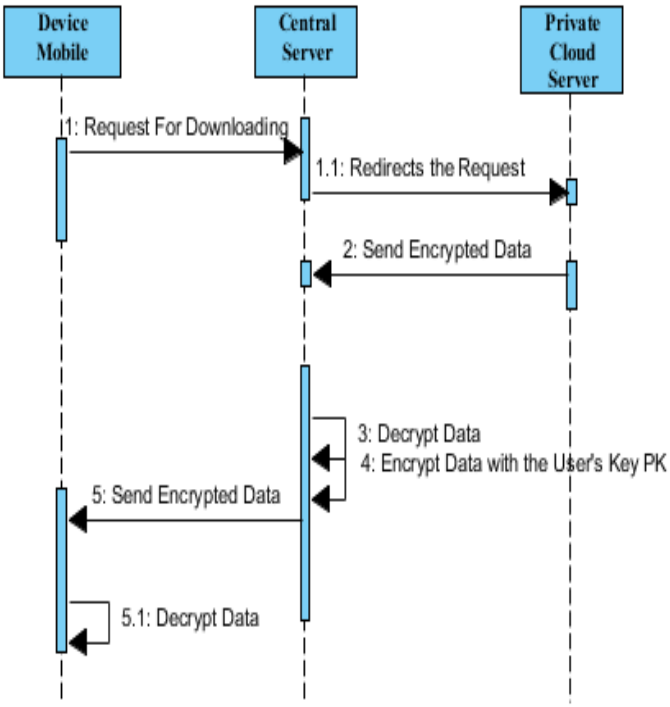

Fig. 4. Downloading Scheme

Our downloading scheme ensures confidentiality and data integrity; it also allows privacy of users because the data stored in the cloud is encrypted. Our scheme uses the services of a private cloud server [20] which increases the level of security and reduces the risk of data loss. The mobile users may be interpreted the received data because they were re-encrypted using the appropriate encryption key for each mobile device.

ISBN: 978-988-19253-4-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

TABLE I
COMPARISON OF SECURITY FRAMEWORKS IN MCC

	Kamara et al. [12] (2010)	Hsueh et al. [13] (2011)	Han et al. [23] (2013)	Zhiwei et al.[14] (2014)	Our Proposed Model
Authentication	NO	YES	YES	YES	YES
Data protection	YES	YES	YES	NO	YES
Encryption	YES	YES	YES	NO	YES
integrity	NO	YES	YES	YES	YES
Homomorphic System	NO	NO	NO	YES	YES
Privacy	NO	NO	NO	NO	YES
Secure Data even after loss password	NO	NO	NO	NO	YES

IV. PERFORMANCE ANALYSIS

A. Security analysis

We will proceed in the following to a security analysis which will allow us to evaluate our security framework compared to vulnerabilities and security threats. We will prove that our structure can tackle all these security issues very efficiently, and offer to mobile users an interface that will allow them to upload and view safely their sensitive personal data stored in the cloud server.

- *Data protection:* Our security framework aims primarily to ensure data security and mobile users privacy. So, all communications between different entities of our structure are encrypted. This is what keeps a high level of security, and only the concerned mobile users can decrypt and interpret data.
- *Authentication and Integrity*: In many cases, it is not very easy to identify mobile users, which can cause serious security problems [21]. To fix this problem we have developed an authentication scheme that enables mobile users to authenticate in order to receive and view their data safely. Several attacks aim to forge valid signatures and compromise data integrity. Our model uses the algorithm proposed by Zhiwei et al. [14] that can forge a robust homomorphic signature to protect data.
- *Threat of a Cloud Service Provider:* Several security problems can arise from cloud service providers, and even if some providers ensure to their clients the protection of their data stored in Cloud servers, it is better not to completely trust their data protection system. Our model uses a homomorphic encryption system to encrypt data before it's been sent to the cloud server. For more safety our structure uses private cloud computing server services to avoid problems related to data collocation and virtualization [22], and to prevent the loss of sensitive data
- *Loss of user identity and password:* The Loss of mobile user ID can be very dangerous. But in our structure, it is imperative to make an authentication request to receive a password PWD and then access the data which is located in the distant cloud server. Thus, the user will have to enter additional data, such as his account number and his phone number. This procedure will prevent mobile users from losing their data even in the case of their ID loss.

B. Evaluation and Comparison

In this section we will evaluate as shown in Table I our model compared to existing models. The purpose of our evaluation is to show that our design satisfies the customer expectations in terms of safety and that it ensures confidentiality authenticity and integrity.

Our evaluation shows that our design satisfies the security requirements, and that allows mobile users to authenticate and retrieve their data safely. Our scheme uses a signature homomorphic which ensures data integrity, and it also helps to protect user data even in the case of loss of password. Using a private cloud server and the encryption of all data ensures the privacy of the users and keeps a high level of security.

V. SIMULATION AND EXPERIMENT

A. Experiment Environment

Practical evaluation is performed in a personal computer, with the following characteristics:

- Intel(R) Core(TM) i7-2670QM CPU @ 2.20GHz (8 CPUs), ~2.2GHz.
- Memory 8192MB RAM
- Intel(R) HD Graphics Family (1696 MB).

We developed our application with java and java android, and we used an android smartphone for testing with the following characteristics:

- Processor dual-core 1.2GHz.
- Memory 1 Go

N.B: We made test on virtual machine before implementing them in real machines.

B. Experimental results

In this part we will propose an implementation of our download structure and homomorphic authentication. We will develop an application which allows mobile users to access their banking information and consult them safely.

We assume that the Bank uses services of a cloud provider to store its customers data. Each bank customer has an ID and password, which allows him to register in the mobile application. Once connected, he sends a request to the Bank local server to access his personal data. The local server sends a new password PWD to mobile user, allowing him to securely access his personal data.

ISBN: 978-988-19253-4-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

TABLE II
TEST OF USE OF OUR SECURITY PLATFORM

Registration : (Mobile Device)	
Login :	Karim.zkik
Password :	110251032
Forging a signature from the personal data of the mobile user: (Mobile Device)	
Account number:	185156753212
ID :	110251032
Phone number:	0615318287
N = p*q:	193105375012785175488407837176022112881
Time of validity :	24 h
Time digest :	1ff1de774005f8da13f42943881c655f
Number of blocs n	10
signature1_1: signature1_2: signature1_3: signature1_4: signature2_1: signature2_2: signature2_3: signature3_1: signature3_1: signature3_3:	718560756192253……130286919974899 635197852275421……200563432254935 244061552333593……961636800483234 847324068849953……124788710851252 365986028155682……896650598164824 621354567605975……532201405198811 101337780267101……986217241841814 763184105730929……644641230225807 438412718836446……987828789067592 836478842306245……472924981807224
signature:	718560756192253253542042 1……64672167522703537847292498 1807224
authentication request	185156753212110251032032061531828 7
Encrypted authentication request PKSC(NC,ID,NP) :	820137745143330002008116545650 2……52553062557862696225600662 700060503758707351
Received data from the mobile user: (Central Server)	
Encrypted authentication request :	820137745143330002008116545650 2……52553062557862696225600662 700060503758707351
signature:	718560756192253253542042 1……64672167522703537847292498 1807224
Forging a new signature from the user ID: (Central Server)	
Time of validity :	24 h
Time digest :	1ff1de774005f8da13f42943881c655f
ID:	110251032
Part of signature 1 Part of signature 2 Part of signature 3	3659860281556824167……572439896650598164824 6213545676059757892……719053532201405198811 1013377802671011838……456816986217241841814
Part of signature on ID	230449297454183799081414456 3……90937462690663996425400824 974896
Checking the validity of the signature and authenticity of the request: (Central Server)	
Computes x from the signature sent by the user:	230449297454183799081414456 3……90937462690663996425400824 974896
final verification :	1
Session Key:	7F45D0E56331A1
Send a request to view our bank balance: (Mobile Device)	
request to view our bank balance :	7F45D0E56331A1 , R1 (R1 is the request to see balance)
Receive Data from the Cloud Server: (Central Server)	
Encrypted Data received from the Cloud:	817531134574057061558714474254556270006417141900101282390103897595818796202358981314369348449217699478767723018337723299374791505526851017251
Decrypt Data with the central server's secret key	1000 Dollars
Encrypt Data with the user's public key	352778882925008839512541055137779122266772031942505739406487102223896716431643652785 1
Send Encrypted Data to Mobile user: (Mobile Device)	
Encrypt Data with the user's public key	352778882925008839512541055137779122266772031942505739406487102223896716431643652785 1
Decrypt Data with the user's secret key	1000 Dollars

ISBN: 978-988-19253-4-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

In the Table II, there is a description of our application use test results.

Firstly we will register in the mobile application, then we will forge a homomorphic signature and an authentication request that we will send to the central server. The central server will check the validity of the signature of the request before sending a session key to the mobile. The mobile user will send a request to see his balance, for example, using the session key. Cloud server will send the required data to the central server, which redirects to the mobile after being decrypted and re-encrypted in such a way that the mobile user is the only one who can interpret them.

VI. Conclusion

Our security structure offers the possibility to fully use the mobile cloud computing services because it allows avoiding the problems related to security. We have demonstrated in our evaluation that our structure ensures the authenticity of users and data protection, and the use of a homomorphic signature allows, on another hand, ensuring the integrity of data and preventing attacks that aim to forge valid electronic signatures. Our structure also allows mobile users to interpret the encrypted data stored in the cloud, even if the data is initially encrypted with the key of the company's central server. We have developed an implementation of our architecture; and we have chosen as an example a Bank that offers online services to its clients, like viewing their balance. This implementation shows that our structure permits secure downloading of data and user privacy.

Given the resource constraints of mobile devices, we project in the near future to make our application more efficient, and more flexible to use, and we plan to develop a homomorphic encryption mechanism that will be able to do calculations on received data before returning them to the distant cloud server.

References

[1] P. N. Dharmale, P. L. Ramteke, "Mobile Cloud Computing" International Journal of Science and Research (IJSR), 2319-7064, 2013.

[2] N. Fernando, Seng W. Loke, W. Rahayu, "Mobile cloud computing: A survey", Future Generation Computer Systems 29, pp. 84–106, 2013.

[3] L. Guan, X. Ke, M. Song, J. Song, "A Survey of Research on Mobile Cloud Computing", Sanya, Hainan Island China, Computer and Information Science, ACIS International Conference on, 2011.

[4] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, Volume 34, Issue 1,pp. 1–11, 2011.

[5] A. Shahzad, and M. Hussain, "Security Issues and Challenges of Mobile Cloud Computing", International Journal of Grid and Distributed Computing Vol.6, No.6, pp.37-50, 2013.

[6] Hoang T. Dinh, C. Lee, D. Niyato, P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches", Wireless Communications and Mobile Computing, Volume 13, Issue 18, pp. 1587–1611, 2013.

[7] A. Nasir Khan, M.L. Mat Kiah, Samee U. Khan, Sajjad A. Madani, "Towards secure mobile cloud computing: A survey", Future Generation Computer Systems 29, pp. 1278–1299, 2013.

[8] A. Patel, M. Taghavi, K. Bakhtiyar, J. Celestino Junior, "An intrusion detection and prevention system in cloud computing: A systematic review", Journal of Network and Computer Applications 36, pp. 25–41, 2013.

[9] Mark D. Ryan, "Cloud computing security: The scientific challenge, and a survey of solutions", The Journal of Systems and Software 86, pp. 2263– 2268, 2013.

[10] D. Zissis, D. Lekkas, "Addressing cloud computing security issues", Future Generation Computer Systems, Volume 28, Issue 3, pp. 583–592, 2012.

[11] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications 34 (1), pp. 1–11, 2011.

[12] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, I. Brandic, "Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility", Future Generation Computer Systems 25 (6), pp.599–616, 2009.

[13] S. Kamara, K. Lauter, "Cryptographic cloud storage", 14th International Conference on Financial Cryptography and Data Security, LNCS, IFCA/ Springer-Verlag, pp. 136-149, 2010.

[14] S.C. Hsueh, J.Y. Lin, M.Y. Lin, "Secure cloud storage for conventional data archive of smart phones", in: Proc. 15th IEEE Int. Symposium on Consumer Electronics, ISCE '11, Singapore, 2011.

[15] Z. Wang, G. Sun, D. Chen, "A new definition of homomorphic signature for identity management in mobile cloud computing", Journal of Computer and System Sciences 80, pp. 546–553, 2014.

[16] M. Ogburn, C. Turner, P. Dahal, "Homomorphic Encryption", Procedia Computer Science 20, pp. 502 – 509, 2013.

[17] D. Pointcheval, J. Stern, "Security Proofs for Signature Schemes", Lecture Notes in Computer Science Volume 1070, pp 387-398, 1996.

[18] Lei Wei, Scott E. Coull, Michael K. Reiter, "Bounded vector signatures and their applications", in: ASIACCS'11, pp. 277–285, 2011.

[19] R. Johnson, D. Molnar, D. Song, D. Wagner, "Homomorphic signature schemes", in: Topics in Cryptology — CT-RSA 2002, in: Springer LNCS, vol. 2271, pp.244–262, 2002.

[20] Private cloud (internal cloud or corporate cloud). Available: http://www.interoute.com/cloud-article/what-private-cloud

[21] Y. Yu, J. Ni, M. Ho Au, H. Liu, Hua Wang, C. Xu, "Improved security of a dynamic remote data possession checking protocol for cloud storage", Expert Systems with Applications 41, pp. 7789–7796, 2014.

[22] J. Han, W. Susilo, Y. Mu, "Identity-based data storage in cloud computing", Future Generation Computer Systems 29, pp. 673–681,2013.

ISBN: 978-988-19253-4-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)