Mobile Cloud Authentication and Secure Communication

R. Gokaj, M. Ali Aydın, R. Selami Özbey

***Abstract*—The secure communication of today's mobile devices is of high interest because the threats have increased and it is now not easy to handle the billions of devices securely. With the ongoing developments of huge systems being transformed into cloud systems, we have the need to provide an easy to use, simple, flexible and robust mobile client platform to be used in the cloud environments. One of the most important challenges that we face is the way to secure the environment. The first step is to secure the authentication, and after that to secure the application communication and file transfer. Here we present a way, by using nowadays technologies like Mobile Signature, SSL, SOA, SFTP and combine them to provide a complete solution for a mobile cloud environment.**

***Index Terms*—About authentication, cloud, mobile, secure communication.**

I. INTRODUCTION

NOWADAYS, mobile devices are being of high interest because of all the actions they can perform. We can say that nearly all the PC operations have been to transferred to mobile devices. So, basically every daily action previously performed only on our PCs can now be performed in mobile devices.

People always feel the need to have with themselves their personal data on which we can give as an example photos, emails, work files, reminders, calendar, music, etc. In order to make this possible for all people all around everywhere, cloud solutions come up for this. In order to have a brief description for cloud computing, we can tell that this is a group of web solutions which offers services that can be accessed through internet.

Manuscript received September 2, 2013. This work was supported in part by the Istanbul University Scientific Research Projects Department with project number 28489.

R. Gokaj, is with the Computer Engineering , Istanbul University, Istanbul, Turkey (e-mail: redigokaj@gmail.com).

M. Ali Aydın, is with the Computer Engineering , Istanbul University, Istanbul, Turkey (e-mail: aydinali@istanbul.edu.tr).

R. Selami Özbey, is with the TUBITAK-BILGEM-UEKAE, Kocaeli, Turkey (e-mail: selami.ozbey@tubitak.gov.tr).

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)
- Storage as a Service (STaaS)

The one which is part of our concept, related with the mobile devices, is the "Software as a Service". So, a shared software will be running on the cloud and make it possible for all clients to use it in a secure way.

When thinking about a cloud solution for the mobile devices, we refer to the term Mobile Cloud. In fact, this should not be confusing by thinking that the cloud environment will run on the mobile devices. The cloud distributed servers will be used as source when the mobile devices (considered as clients) can be connected and utilize the service or the platform. With mobile devices being part of the cloud environment, confidential data may be by mistake exposed to unauthorized people. This means that a security threat may be part of the system's solution. So a secure cloud environment should offer a reliable connection and operational process when dealing with mobile devices.

II. RELATED WORKS

As an example of current cloud authentications we can see Amazon EC2. It offers a public / private key authentication in order to connect with the server running on Amazon's cloud. Regarding the technical overview of implementing the cloud connections over a mobile device we have got a very detailed explanation in the manuscript "Mobile cloud computing: A survey" [1]. It is stated that limited resources from mobile devices make it obligatory to share common resources among cloud computing. The simplest example with a basic approach would be using the Gmail application on your mobile phone.

- In this case we face may problems like:
- Phishing attacks
- XML signature element wrapping
- Man-in-the-middle attack
- Eavesdropping
- Brower-based authentication weaknesses

These problems are specified in "Considerations for mobile authentication in the Cloud" [2] where general security issues are given as an example. The proposed security checks go deep into the SIM card on which we take guarantee that it is not corrupted or accessed without permission. That's why also in our proposed approach, the SIM card's digital signature operation helps us in the authentication stage.

In order to ensure the identity of a device user, the Digital ID term takes place [3]. In cooperation with the mobile line carrier, the new properties of 128 bit SIM cards are used. A special software runs on that SIM card. This software allows the user to sign information and send it back to the carrier line. Because the card is specially produced by the carrier, the carrier is able to know if the signature is correct or not.

Data theft [4] is another problem which should be considered to be solved inside the server side part of the cloud. Specific file organizations should be done in the part where users' data is stored. In this case, the cloud environment should protect each user's data and not allow unauthorized access.

Authentication modules [5] should be separated and considered as a standalone module which operates independently and securely. This shows the importance of the authentication process over a cloud environment.

By running mobile applications on a cloud [6] some other topics should be considered as very much important.

- Application re-design and deployment
- Network condition and service availability
- Control of applications
- Privacy of data
- Information security

Another approach of securing the authentication is TrustCube [7]. This consists of a collection of SMS and Call history and encrypt them with a hash algorithm. After that, check this data with the previous history stored in the cloud part. In this case, if authentication is done from another device, it would be noticed immediately.

Regarding the commercial applications used for cloud data synchronization we may consider DropBox and Google Drive. Basically, after a username/password authentication, a file sharing service is enabled. This makes possible for you to access your shared files in every device that you have setup with the cloud environment. If we have to specify the service that these two providers offer, we can tell it is STaaS (Storage as a Service).

III. THE PROPOSED METHOD

The main theme can be divided into some specific topics which can later be considered alone. We have to consider:

- Authentication
- Application Communication
- File transfer

As given in Fig. 1, we have the big picture which represents the mechanisms required for the full cycle to be implemented. In the proceeding sections the big picture will be divided in small parts and an explanation will be given for each part.

A. Authentication

1. The user makes a classic authentication with username & password.
2. The server generates a session key SKEY.
3. We need to be sure that this SKEY will be used from our trusted device which has the CA trusted identity.
4. So, Mobile Signature is used to check the session key if it is being used from the real trusted mobile device. This key maybe validated periodically during the mobile-cloud communication.

Part of the authentication mechanism is also the session handling. The provided SKEY will be binded with the session stored in the server for the current connected client. In order to protect the sequence of web service calls, we put a SEQUENCE_NUMBER and initialize it with 1 and after the after each request we increase it by one. If the sequence number's chronology is broken, then the authentication fails and is required to be done again. If in any case SKEY expires or there is a problem with the session, then the server informs the client that authentication should be refreshed and blocks in the server all the operations until the authentication is done again. Here SKEY should not be confused with SSL. The SKEY is only the representative of the client in the server instance.

B. Application Communication

The client will communicate with the server using a basic web service approach. In this case we say that we use SOA (Service Oriented Architecture) platform. In order to secure the communication we need to use SSL in order to encrypt the traffic. HTTPS protocol will be used in the cloud (server side) and the client will be able to connect by using the signed certificates.

C. File transfer

A very good way for file transfer is the SFTP protocol. Secure authentication and transfer take place in this protocol. A public / private key pair is generated from the server and the public one is given to the client. The client then, uses this public key to connect and make the file transfer (while the private key stays only on the server).

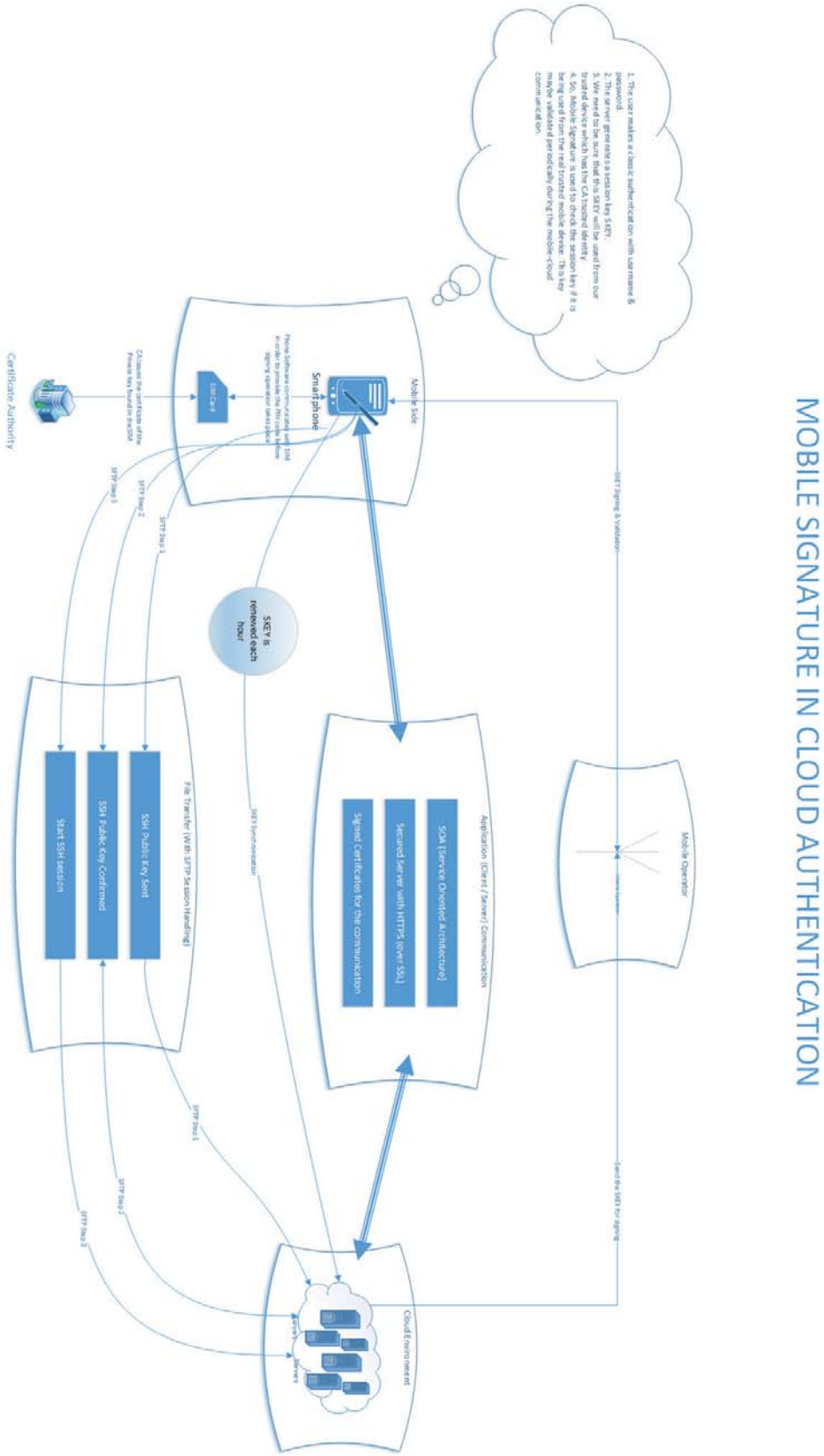

Fig. 1. Securing the authentication and file transfer in the mobile cloud

TABLE I
NOTATIONS

Notation	Explanation
AMO	Authorized mobile operator
MSgReq	Mobile signature request
MSsHash	Mobile signature hash key
SKEY	Session key
SN	Sequence number
WSReq	Webservice request
SSLe	SSL encryption
WSRes	Webservice response
SSs	SSH start session
SP_{KR}	SFTP public key request
SP_{KC}	SFTP private key check
FP	File transfer progress
SSe	SSH session end
MSpin	Mobile signature pin code check

D. Schema explanation

Fig. 1 is the overall system that shows how information travels from the mobile device to the cloud and vice versa.

In Fig. 2, we see the server side application structure. Application communication is done via HTTPS protocol, which has a SSL secured layer with a signed certificate. SOA architecture means a communication with web services. So, our mobile device will call web services found in the server side. Regarding file transfer, SFTP structure is given in the picture. By this way, the file transfer, which is an expensive network operation, will be handled by this protocol.

In the next picture, Fig. 3, we see the mobile phone and the SIM card which does the signature process by using the Digital ID information. The mobile device communicates with the carrier and via internet it communicates also with the

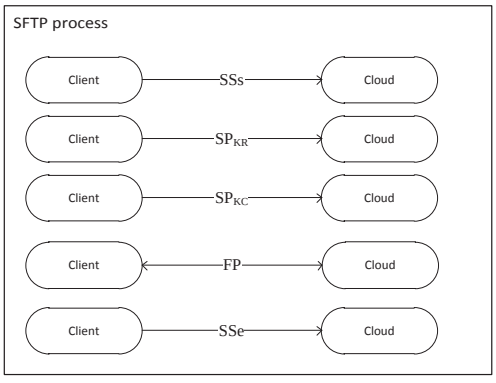

Fig. 4. The SFTP file transfer progress step by step

cloud environment by doing authentication, application access and file transfer. As the SIM Digital Signature is protected by law, it gains an official trust level.

The Fig. 4 shows our cloud environment which is a distributed system of servers that contain the SFTP module. All SFTP steps are described there where it is obvious that file transfer is totally independent from the application module.

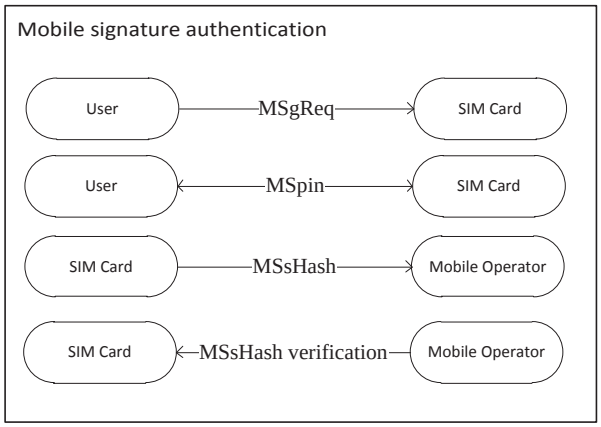

Fig. 2. Steps that a mobile device follows up in order to have a secure authentication via Mobile Signature

A key feature of this system should be the uptime guarantee

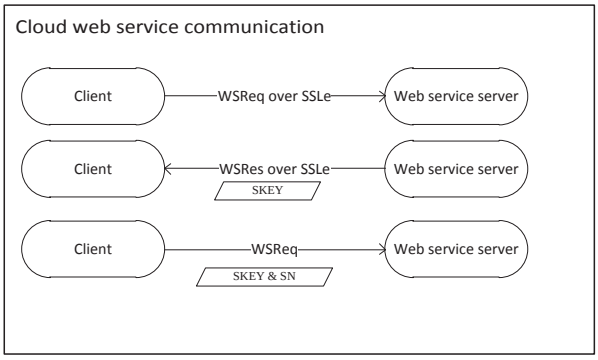

Fig. 3. The secured file transfer and application business communication

in any failure condition of one of the servers. So, the distributed application should work on all servers and if any of the servers goes down, another server should continue operating without interrupting. So, distributed session handling is present in this environment.

Creating this system in the real world is possible as the environments and tools below can be easily used. According to the researches done, the Amazon EC2 (offered by Amazon Inc.), is suitable as it offers: The Elastic Cloud, Virtual Load Balancers, Cloud Storage and Backup.

The Mobile Signature is officially offered by Turkcell in Turkey, and it is protected by electronic signature law number 5070. Another reason to use this Mobile Signature is that Turkcell is one of the first companies in the world that designed and developed the Mobile Signature.

As a comparison with the previous works done at [8], results are shown at Table II.

TABLE II
COMPARISON ACCORDING TO ATTACK TYPES

Attack	Proposed Model	Method at [8]
Man-In-The-Middle	Supported by sequence number	Not supported
Identity theft	Supported by Mobile signature	Not Supported
Phishing	Supported by Mobile Signature	Supported
Eavesdropping	Supported by Session Key and HTTPS	Supported

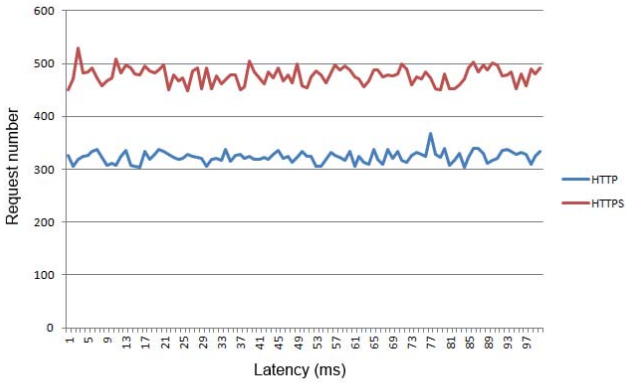

Fig. 5. The SFTP file transfer progress step by step

Also, a comparison graph is prepared in order to tell the difference of running an application over HTTP and HTTPS. In Fig. 5 the graph shows 100 requests made to a test server running firstly in HTTP and after that in HTTPS. There is a difference of about 150 milliseconds which in fact is not event distinguished by the user. In the other hand, this latency is related with the protection mechanisms running in the proposed model.

IV. CONCLUSION

By this material, we show how a secure authentication can be implemented on a real life platform currently supported by most of the mobile operators. We mentioned all types of required protocols in order to handle a complete infrastructure for an application to be connected to the cloud and operate. All the technologies gathered all together already exist, but in this platform all of them are combined in such a way that provides a secure and flexible operating environment.

The user identity is assured by the Mobile Signature. This makes possible to track the real person of each operation. By using SSL in the middle, the communication channel is secured. The session key and the sequence number make it impossible for a MAN-IN-THE-MIDDLE to replace or retry the network message.

REFERENCES

[1] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: a survey". Future Generation Computer Systems, May 2012.
[2] Z. Ahmad, K. E. Mayes, S. Dong, and K. Markantonakis, "Considerations for mobile authentication in the cloud". Information Security Technical Report 16, 2011, pp. 123 – 130.
[3] M. Whitehead, "GSMA Europe response to European Commission consultation on eSignatures and eIdentification", April 2011.
[4] D. Suna, G. Changb, L. Suna, and X. Wanga, "Surveying and analyzing security, privacy and trust issues in cloud computing environments". Procedia Engineering 15, 2011, pp. 2852 – 2856.
[5] W. Tang, J. Lee, B. Song, Md. M. Islam, S. Na, and E. Huh, "Multi-platform mobile thin client architecture in cloud environment". Procedia Environmental Sciences 11, 2011, pp. 499 – 504.
[6] S. Hung, C. Shih, J. Shieh, C. Lee, and Y. Huang, "Executing mobile applications on the cloud: framework and issues". Computers and Mathematics with Applications 63, 2012, pp. 573–587.
[7] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, and E. Shi, "Authentication in the clouds: a framework and its application to mobile users". Management of Computing and Information, October 2010.
[8] S.N. Hsueh, J.J. Lin, M.Y. Lin, "Secure Cloud Storate for Convenient Data Archive of Smart Phones", IEEE 15th International Symposium on Consumer Electronics, 2011, pp. 156-161.