IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

An Authenticate Cryptography based security model for handling multiple request from multiple devices for Mobile Cloud Computing

Debabrata Sarddar[1], Enakshmi Nandi[2]

Assistant Professor, Department of Computer Science & Engineering, University of Kalyani[1]

Research Scholar, Department of Computer Science & Engineering, University of Kalyani[2]

Abstract: Mobile Cloud Computing (MCC) has revolutionized the way in which mobile endorsers across the globe leverage services on the go. MCC integrates cloud computing into the mobile environment and get over the obstacles related to performance (e.g. battery life, storage, and bandwidth), environment (e.g. heterogeneity, scalability, availability) and security (e.g. reliability and privacy).It is an answer to intensive processing and storage demand of real-time and high end applications. The capabilities of mobile devices have been amending very quickly in terms of computing power, storage, feature support, and developed applications. Even these mobile applications are still intrinsically limited by a relative lack of bandwidth, computing power, and energy compared to their connected counterparts. In this paper we systematically explore the privacy and security issues and launch a cryptography based model for handling multiple request from multiple devices for Mobile Cloud Computing. Our approach helps to authenticate communication between customers and service providers using encryption, decryption and message digests.

Keywords: Cloud Computing, Mobile Cloud Computing (MCC), Authentication Server (SS), Authentication, Encryption, Decryption, Message Digest.

1. INTRODUCTION

We are existing in a compelling new era for mobile computing. Technological innovations are occurring at an accelerated rate: (1) increasingly, mobile devices are much more capable in terms of processing speed and storage; and (2) the wireless network is becoming much faster and has lower latency, with new deployments such as LTE shaping the field. Parallel to these innovations, cloud computing has soared in popularity. The cloud computing paradigm offers a novel approach for utility computing with unprecedented resource flexibility, agility, and scalability [1]. As Combination of cloud computing and mobile computing, Mobile Cloud Computing (MCC) is a new research topic since 2009. Mobile Cloud Computing has three components, mobile device, wireless communication channel and cloud. Mobile devices have resource constraint in terms of battery power, processing power, memory, and have various types of hardware, operating system, and input -output interface [2]. Security and privacy issues in mobile cloud computing (MCC) are inherited from cloud computing and mobile computing. Due to resource constraints, heavy security algorithm can't be run on mobile device. Mobile Cloud computing providers have numerous security services in place like scanning, authentication for mobile clients, malicious code detection etc. Various services from several providers can be integrated quickly through the cloud to fulfil today's complex client demands. Now a day mobile users seamlessly utilize the cloud to obtain the resource benefits without receiving delays and jitter and without concerning about energy.

Figure1. shows the mobile cloud architecture.

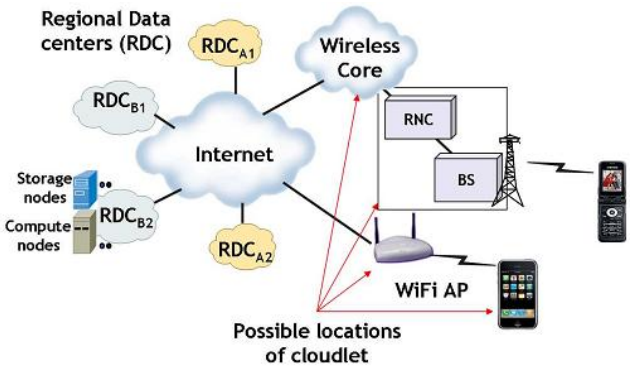

Fig: 1: Mobile Cloud Architecture

This paper throws light on security issue based on cryptography for handling multiple requests from multiple devices for Mobile Cloud Computing.

2. RELATED WORK

Security and privacy issues of MCC have been discussed by many researchers. J. Oberheide et al. [3] proposed Cloud AV platform, malware detection system. In this architecture, mobile agent first analyses the malicious file. If its signature is not matched with the cached database, it is sent to the network service for analysis with the help of multiple detection engines running parallel on host machines with the help of virtualization technique. These techniques have the advantage of better detection of malicious software, reduced on device software

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

complexity and power consumption but suffer from limitations of disconnected operation and accidental privacy hazard. S Zhang et al. [4] presents security framework which adapts mobile device with changing workloads, performance goals and network latency by migrating processing weblets between cloud and mobile device. They raise this model by trustworthy weblets container, Authentication and secure session management, Authorization and access control of weblets, Logging and auditing behaviour of weblets to form more secure framework. Although security during weblets migration can be improved Wang and Wang [5] have proposed framework that uses cloud for providing number of live clients in region based on historical data saved in cloud which helped in minimization of processing and communication overhead in cloud but doing spatial cloaking based on historical data can lead to privacy loss. The cloaking in mobile device increased processing overhead and energy consumption. Huang et al. [6] presents framework – Mobil Cloud in which the secure computation is done with three domains (a) cloud mobile and sensing domain (b) cloud trusted domain and (c) cloud public service and storage domain. In cloud we have multiple replica of Smartphone which can detect several types of attacks in parallel. H.Zhang and X Mingjun [7] proposed distributed spatial cloaking in which distributed anonymity having location information for cloaking. Distributed anonymity can handle frequent requests from users without being bottlenecked. P.Zou et al. [8] proposes Phosphor in which interaction between Sim card and Digital Rights Management Agent has been protected by the License Status Word protocol. Saman Zonouz et. al. [9] proposed Secloud; a cloud based comprehensive and lightweight security for smartphones. Secloud runs the emulators of Smartphones in cloud which provide security to mobile device by security analysis of data in mobile device. In this architecture cloud assumes to be fully trusted which needs to be reconsidered .The personal data of clients accessed to the cloud can affect the privacy issues. Cloud Computing is an open environment, so any weakness can cause security risk of the whole system.

There a four important types of security services:

Authenticate: Suppose a sender sends some data to the receiver. Authentication means receiver will get the data coming from the authenticated sender, no other third party cannot claim to be sender [10, 11]. So it is an assurance that the communicating data is same as the data sends by the sender.

Data Confidentiality: By the term confidential it can be said that the data is hidden from any third party. Only the sender and receiver are able to access the data, not anyone else [10][11].

Data Integrity: The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay) [12, 13].

Non Repudiation It provides protection against denial of services by one of the entities involved in a communication of having participated in all or part of the communication [10].

Cryptography is the practice and study of hiding information. Cryptography referred almost exclusively to encryption, which is the process of converting the plaintext into unintelligible gibberish i.e., cipher text. Decryption is the reverse, in other words, moving from the unintelligible cipher text back to plaintext.

Symmetric Key Cryptography: Symmetric encryption is one type of cryptosystem in which one key is used for both encryption and decryption [10, 13]. For example DES Cryptography.

Asymetrix Key Cryptography: Here two different key is used, one key is used for encryption (public key) and other key is used for decryption (private key) [10]. Assume, each entity possess a set of (private key, public key) pair. One popular algorithm to calculate this type of key pair is RSA algorithm [10] describes below:

Select two large prime number p and q ($p \neq q$)
Calculate $n = p * q$ (14)
Calculate $\emptyset(n) = (p - 1) * (q - 1)$
Select integer e (encryption key) such as
$\gcd(\emptyset(n), e) = 1; 1 < e < \emptyset(n)$
Calculated d (decryption key) such as

$d = {}^{e-1} \pmod{\emptyset(n)}$

Encryption by B
Cipher text: $C = M^e \bmod n$

Decryption by Alice with Alice's Public Key
Plaintext: $M = C^d \bmod n$.

3. PROPOSED METHOD

In this paper we want to focus on security issues for handling multiple requests from multiple devices at a time on mobile cloud Computing. There may be a chance of attackers, hackers, third party intruder or others to interrupts this communication. This is a vital problem of handling multiple requests in mobile cloud computing. To perform an intact security based communication we proposed a cryptography based model. According to proposed model, Cloud Service Provider (CSP) is a trusted authority and is responsible for all decisions and activities. Authentication Server (AS) and Storage Server (SS) are two organizations under the supervision of CSP and their functions and activities are controlled by CSP. First of all the CSP, AS and SS maintain a model which is solely dependent on a set of Public Key and Private Key. Now the second constraint is Public key of CSP is open to all, and only CSP knows the Public key (14) of AS and SS. So no other third party can use the Public Key, only CSP is able to use the Public Key of AS & SS, but if any third party wants to communicate with AS or SS, then she has to communicate with CSP first. If CSP grants the third party to communicate with the AS or SS, then she can do so. In this model the third party never knows the Public Key of AS or SS but she can securely communicate with them. Three layer of security checking is performed to ensure authentication. In the 1st phase, customer sends a request to CSP then the connection will be established between customer/third party and CSP, in the 2nd phase AS verifies the previous connection and authenticates the

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

customer. In the last phase, customer receives information about Storage Server (SS) and communicates with SS.

3.1. Working Principal

To ease of understand, we use some notation to describe our model. We discuss each phase elaborately and describe the notations when they are needed.

1st phase:

Suppose, customer sends a package to CSP including the following information and objects:

User's login information
User's public key
User's current location

User's id which is encrypted by CSP's public key, where user's id may be voter card number or SSN number that uniquely identify the user. User's id will be denoted as user id.

Time-Stamp (TS)

User always remembers his/ her Time-Stamp (TS) and waits for CSP's response[14]. When CSP receives the package, CSP first decrypt user-id using its private key and searches its database against the user-id to check whether the customer is fake or not. If the customer is verified positively, CSP does a set of action as follows.

CSP Enlist the Customer's Name.

CSP calculates message digest (M) of user-id using some standard message digest algorithm (MD5 or SHA1). M= message-digest (user-id) Now, user stores M against username, note if somehow an attacker is able to access the Database of CSP, he will find the message digest of user-id in spite of original user-id. CSP creates two session keys K1 and K2. Encrypt K1 by AS's public key, encrypt K2 by SS's public key. We already discussed that only CSP knows the public key of AS and SS.

Let, $A = E_{pub\text{-}AS}(k1)$
$B = E_{pub\text{-}SS}(k1)$

CSP calculates two time intervals T1 and T2, in which the customer communicate with AS and SS, where (T2>T1).

Let, P1= address of AS,
P2= address of SS,

CSP now sends some information so that customer can securely communicate with AS and SS.

Let, X= [A+ (TS+T1) +P1]
Y= [B+ (TS+T2)]

CSP encrypts X and Y using customer's public key and sends to customer.

CSP encrypts [P2+M + (TS+T1) + (TS+T2) + user's public key] using AS's Public key and sends to AS.

2nd Phase:

After receiving the packet information from CSP the customer decrypts all the packet and retrieve all the information. Then customer finds the address of AS (P1) and the time limit to create connection with the AS and SS (T1, T2) but cannot open A and B, as she is unknown about the public key of AS & SS. Customer now calculates the message digest of his user-id (M1) and after that she creates a package including the following data,

Z= A+M1 + TS' (current time-stamp)

And sends it to AS, as she now knows the address of AS.

AS already receives the packet send by CSP and retrieves all the data by decrypting its private key. After receiving the packet, AS does the following action: AS checks if TS+T1<TS' or not that is the time limit is over or not, if so, AS replies customer as time out message and ask her to log in again. If customer packet reaches within time interval, AS checks A which is encrypted by its own public key, which is known to CSP only, but not to the customer. So it is the same customer who communicates with CSP. There may be a number of customers who creates communication with CSP, so AS further matches M and M1, two messages digests –one received from CSP and another from customer.

When all the checking are done positively, AS now creates a session key K3, encrypt it with SS's public key, and creates a data packet:

$$W= [Ep_{ub\text{-}ss}(K3) +P2]$$

AS sends W to customer. AS sends encrypted M along with (TS+T2) using SS's public key and send it to SS. When the customer again receive the data set from AS, the customer retrieves all the data using its private key. Again the customer finds the address of the storage server, but cannot open K3, the customer, again creates another packet containing encrypted K3, B, M1 (message digest of user-id) and current time stamp (TS) are send to SS. SS receives the packet from customer, finds encrypted K3 and B by its public key; and does the following: S checks if TS">TS+T2, that is if the time limit is expire or not. If yes, SS asks the user to log in again. B is encrypted by CSP; so it is the same customer who has communicated with CSP and now communicating with SS.

K3 is encrypted by AS, so again the same customer who is communicated with both AS and SS. What will happen if some attacker is able to hack both B and encrypted K3? This scheme is still Secure as the attacker cannot have the user-id of the original customer, so he cannot calculate the M1. Thus, SS now matches M' with M receive from AS.M finally, all the authentication checking is performed and SS informs CSP that the customer whose message digest of user-id is M, authenticated securely. CSP then informs the customer that she successfully logged in and asks the customer to follow SLA instructions and one time password to communicate with SS.

4. RESULT AND ANALYSIS

In this Section, we present use of every component used in this model and also describe some odd situations and how they are overcome using this model.

The customer obtains the CSP's public key.

CSP is a well-known authority, so it is obvious that everybody who wants cloud services from CSP must know the public key of CSP, as it is public for everyone.

The customer sends his public key to CSP.
There are a number of users who needs cloud service. But CSP is unaware about them until they send their log in information with her public key.

The customer sends her user_id.
How the CSP knows this it is the original customer who is claimed, so customer sends her id, encrypted by CSP's public key. So, only CSP now able to open it, then check its database and authenticate the customer.

CSP stores message digest of user_id.
User_id is the only key to authenticate a unique customer so instead of storing the user_id, CSP stores the message digest (M) of user_id in its database. If anyone is able to find, he will get the M, not the original user-id.

How the customer is authenticated between AS and CSP?
CSP creates K1 and encrypted using AS's public key (A). So, only AS can open it. Customer sends A to AS, and A can be created only by CSP, hence it is the same customer.AS match's two message digest of user_id, M and M1, one received from CSP and another from customer.

Customer gets the address of AS (P1) from CSP. How the customer is authenticated between AS and SS?
AS creates K3 and encrypts using SS's public key. SS's public key is known to AS, but not to the customer. Thus when customer sends the encrypted K3 to SS, authentication checking is done.

SS matches two message digest of user_id, M, M1, one received from AS and another from customer.

Customer gets the address of SS (P2) from AS. How the authentication is verified between CSP & SS?
CSP creates K2 and encrypts it using SS's public key (B). SS receives it from customer.

5. CONCLUSION AND FUTURE WORK

So far in this paper, we introduce a model to ensure authentication when a user creates a connection with CSP. Here we will try to use more complex encryption process like AES, El Gamal encryption technique, elliptic curve encryption to provide cloud security. In this above approach, we assume that the customers wish to connect with single storage server (SS). In my previous work (15) I have already described how multiple requests can handle with an optimized routing algorithm, here we demonstrate a security based model for an intact communicative process. In future we will try to add data integrity and confidentiality in the described future works.

REFERENCES

[1] M. Armbrust et al. Above the clouds: A berkeley view of cloud computing. Technical Report UCB/EECS-2009-28, UC Berkeley, 2009.

[2] "Privacy and Security in Mobile Cloud Computing: Review" by Sapna Malik ,GGSIPU University Delhi, India, MM Chaturve di Ansal University Gurgaon,India," International Journal of Computer Applications" (0975 – 8887)Volume 80 – No 11, October 2013

[3] Oberheide, J., Veeraraghavan, K., Cooke, E. and Jahanian, F.2008, Virtualized in-cloud security services for mobile devices. In Proceedings of the 1st Workshop on Virtualization in Mobile Computing (MobiVirt), 31- 35.

[4] Zhang, X., Schiffman, J.,. Gibbs S, Kunjithapatham, A., and Jeong S.2009,Securing elastic applications on mobile devices for cloud computing. In Proceeding ACM workshop on Cloud computing security, CCSW '09, Chicago, IL, USA.

[5] Wang, S .and S. Wang X.," In-device spatial cloaking for mobile user privacy assisted by the cloud", in Proceeding 11th International Conference on Mobile Data Management, MDM '10, Missouri, USA, May 2010.

[6] D. Huang, X. Zhang, M. Kang and J. Luo," MobiCloud: building secure cloud framework for mobile computing and communication," in Proceeding 5th IEEE International Symposium on Service Oriented System Engineering, SOSE '10, Nanjing, China, June 2010.

[7] H. Zhangwei. and X. Mingjun," Distributed Spatial Cloaking Protocol for Location Privacy," in Proceedings of the 2nd International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), vol. 2,June 2010, pp. 468.

[8] P. Zou, C. Wang, Z. Liu , and D. Bao, " Phosphor: A Cloud Based DRM Scheme with Sim Card," in Proceedings of the 12th International Asia-Pacific on Web Conference (APWEB), June 2010,pp. 459.

[9] Saman Zonouz, Amir Houmansadr, Robin barthier, Nikita Borisov,William Sanders,"Secloud:A cloud based comprehensive and lightweight security solution for smartphones," published in Science Direct journal of Computers and security ,Volume 37, 2013, pp. 215-227.

[10] S. William, "Cryptography and Network Security Principles and Practice Fifth Edition" Pearson, BBS, (2011).

[11] K. Jashanpreet Pal, K. Rajbhupinder, "Security Issues and Use of Cryptography in Cloud Computing ", International Journal of Advanced Research in Computer Science and Software Engineering ISSN: 2277 128X vol. 4, issue 7, (2014) July.

[12] S. Joachim, "Cloud Services", 4th IEEE International Conference on DEST, Germany, (2010).

[13] D. Akansha, K. Janda Harneet, B. Sayalee, "Security on Cloud Using Cryptography" International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, issue 3, (2015) March ISSN: 2277 128X.

[14] "An Authenticate Model of Cloud Interaction Using Cryptography" by Debabrata Sarddar, Nilanjana Das and Joy Halder , International Journal of Grid Distribution Computing Vol. 8, No.6, (2015), pp.9-18 http://dx.doi.org/10.14257/ijgdc.2015.8.6.02

[15] "A new Approach on Optimized Routing Technique for handling Multiple request from multiple devices for Mobile Cloud Computing" by Debabrata Sarddar, Enakshmi Nandi,"International Journal of Computer Science and Mobile Applications"Vol.2,Issue 8,August 2015,pg 50-61,ISSN: 2321-8363