PROTECTING THE ENCRYPTION KEY FOR SECURE COMMUNICATION IN MOBILE CLOUD COMPUTING

Abdul Basit Khan*, Yan Guang Hui, Ruksudaporn Wutthikarn,Yang Shuo Wen
School of Electronics and Information System Engineering
Lanzhou Jiaotong University, Lanzhou, P.R.China
Email: pearl1spears@gmail.com

ABSTRACT: *These days we use mobiles, tablets & computers to connect with clouds and use their services. The use of mobiles have increased a lot, almost everyone owns a mobile, pad or tablets and we use mobiles to stay connected to the world and surly our private data also travels through the network from mobile to the cloud or from cloud to the mobile. All communication with cloud occurs through the network. Thus the security of mobile communication has become very important. Cryptography is used to secure the data, multiple cryptographic algorithms like AES, RSA, DES, Blowfish, Elliptic curve and others are available. These algorithms ensure that the data is secure but we don't have any method to ensure that the key traveling over the network is also safe. This paper will describe that how we can add an additional layer of security over the data by encrypting the key. In this way it will become extremely difficult for any intruder or attacker to get any personal information present in cloud or which is being transmitted between cloud and mobile. Our main aim in this paper is to make communication in mobile cloud computing more secure. In this paper we will use AES for data encryption and Vigenère Cipher to encrypt key to ensure maximum security. An additional idea to use mac-authentication is also briefly discussed.*

Keywords: mobile cloud computing, encryption, communication security

1.0. INTRODUCTION

Cloud computing means utility computing over the internet, where you can pay to use software, platform or infrastructure. Mobile cloud computing means that, we can use facilities of cloud from our mobile devices through the software or apps installed on it, actually mobile acts as a client of the cloud. Cloud computing provides three different type of services which involves software, platform and infrastructure. We can take benefit from the cloud in any of these forms. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) (Figure 1). SaaS provides software which clients can use, for example e-mail, games, content management system etc. PaaS provides platforms like a web server, database, development tools etc. IaaS gives us access to the underlying infrastructure of the cloud and we can use virtual machines, network, load balancers etc.

Mobile Cloud Computing (MCC) in simple words refers to a platform or an infrastructure where everything happens outside the mobile, e.g. data processing and also data storage. The Cloud Computing applications has moved away the data storage and the computing power from mobile devices and put everything in the cloud, and it has brought the Mobile Cloud (MC) and its application to the mobile device users (Figure 2). As from the concept of Mobile Cloud Computing (MCC), a general architecture of MCC can be seen in Figure.2. Mobiles or related devices are connected to the networks via base stations which controls and establish the links interfaces between mobile devices and the network. When mobile users' request for some services, the users' information e.g. ID and requests for the services are sent to the central processors which are connected to the servers providing network services. Here some of the services are provided to the users such as authorization or authentication based on the data stored in the data bases. After this, the users' requests are sent to the cloud data bases through the internet and in the cloud, there are cloud controllers that processes and provide the users' with the corresponding services.[1]

As the data is stored on a remote server and there are different possible threats that can affect the data, for example

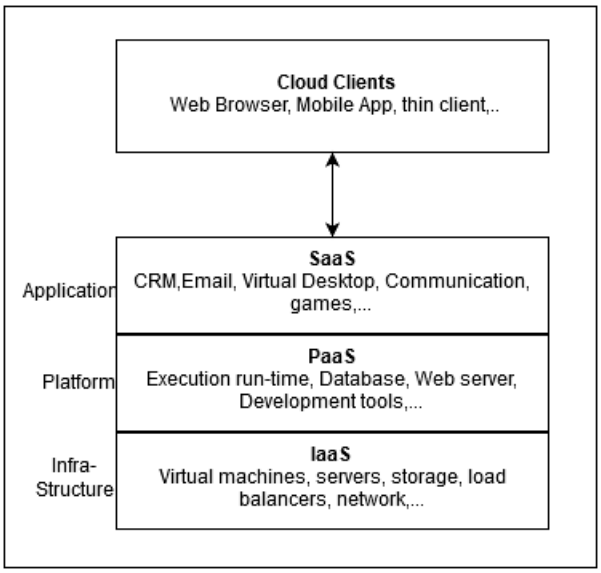

Figure 1: Services of cloud in layers. On top we have SaaS then PaaS and at end IaaS

unauthorized access to data, modification of data, deletion of data, leaking of personal information etc. When data is traveling through the network an intruder can spoof the data. A connection over the internet can be considered a secure connection if an attacker can't access or damage the communication and the attacker fails to launch an active or passive attack (Figure 3). While a connection over the internet can't be considered a secure connection if an attacker can access or damage the communication and the attacker succeeds to launch an active or passive attack (Figure 4). In passive attack the intruder breaks into the communication and starts to listen to the communication or watches the data being sent from one place to another silently without letting anyone know that he/she is doing it (Figure 5). In active attack the intruder breaks into the communication and starts to manipulate or change the messages of communication or modifies the data being sent from one place to another

silently without letting anyone know that he/she is doing it. (Figure 6)

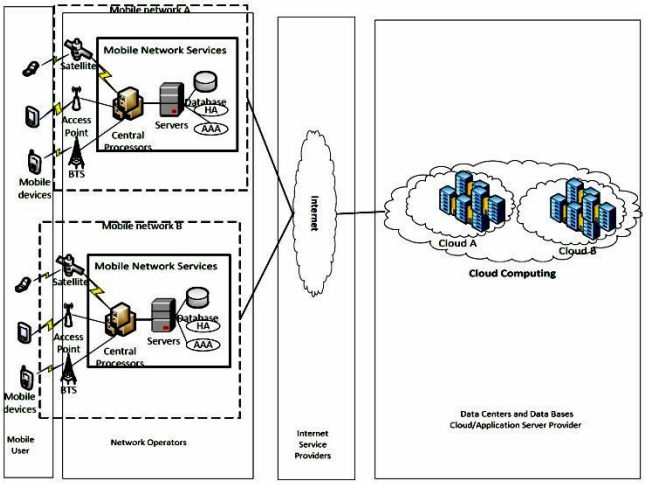

Figure 2: Mobile Cloud Computing Architecture [1]

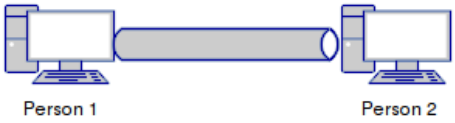

Figure 3: Secure Connection

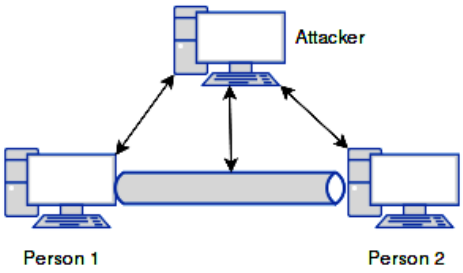

Figure 4: Insecure Connection

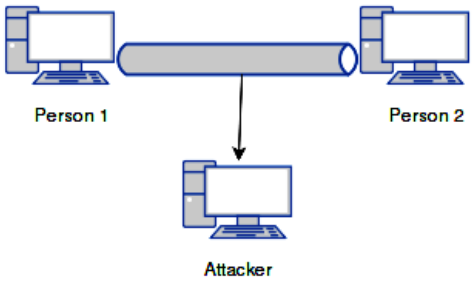

Figure 5: Passive attack, attacker is listening to the communication of person 1 and person 2

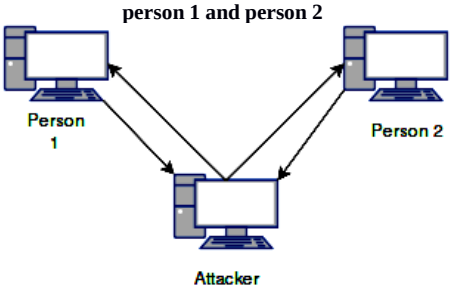

Figure 6: Active attack, attacker is listening to the communication of person 1 and person 2 and changing their messages as he/she wants

Further threats can include Dos attacks, malware, virus, spyware, trojan horse etc. Cryptography is used as a protective measure to ensure security. Cryptography is used to protect the data, during communication and also when it is stored on a remote server. In cryptography data is encrypted on one end and decrypted on the other end. Data without encryption is called plain text and after encryption we call it cipher text. There are two types of encryption, symmetric encryption and asymmetric encryption. In symmetric encryption a secret key is used to encrypt and decrypt the data on both sides. While in asymmetric encryption there are two keys, public key and private key, actually it is a pair of keys. Public key is made publicly available and if A wants to send secret message to B then A will use public key of B to encrypt the data and then send it to B. On the other side B will use its private key to decrypt the message.

We will be using symmetric cryptography in this paper and encrypt its key to make it more secure. We have to encrypt the key because there are different key related attacks like open key model and known key distinguishing attack, these can make our communication insecure. It can help an attacker to decrypt encrypted cipher texts. So, if we encrypt our key as well, then even if attacker gets both key and cipher text he/she will not be able to decrypt data.

2.0. RELATED WORK

[2] have highlighted five security threats to the mobile cloud computing which are DoS attack, XML signature element wrapping, malware injection, mobile terminal security issues and data storage issues. They proposed to use Rest API along with encryption in mobile cloud computing to ensure full security.

[3] have concluded in their paper that the use of mobile cloud computing will increase in future because of its multiple advantages and further mobile cloud computing offers storage and processing power a mobiles which themselves a limited storage and small processing power. Currently there are security related issues which are becoming a hindrance in adoption of mobile cloud computing as people are highly concerned about their privacy.

[4] highlighted that a survey published by International Data Corporation (IDC) in 2009 shows that 74% of Chief Information Officers (CIOs) and IT managers think that security related problems are the main reason because of which organization are hesitating to adopt cloud computing. They also highlighted that a survey by Garter shows that 70% of Chief Technology Officers (CTOs) have shown concerns about security and privacy issues of cloud.

In cloud computing the responsibility of security is upon both the cloud service provider and the cloud service user. The cloud service provider is responsible for ensuring the security and protection of the infrastructure and platform of the cloud while the cloud service user has to take all possible measures to ensure that data is secure. In case of SaaS the security responsibility of cloud service user is to ensure data is secure and application or the software is also secure. While other things in SaaS like compliance, over all security and liability all these are defined in the contract [5].

Mobile Cloud computing security is divided into two types

first is security of mobile user's network and second is security of information present on the cloud. Mobiles have limited processing power as compared to computers thus protecting them using only antivirus is not very effective. Further privacy issues like user's current location and other important information traveling through the network remains at risk of being hacked. On cloud's side we have to ensure integrity, authentication and digital rights management [15].

Results of survey by IDC in 2010 has ranked security challenges as follows

- Security : 87.50%
- Availability : 83.30%
- Performance : 82.90%
- Lack of interoperability standards : 82.20%
- On-demand payment model may cost more : 81%
- Bringing back in house may be difficult : 79.80%
- Hard to integrate with in house IT : 76.80%
- Not enough ability to customer : 76%

This shows that the major challenge is to provide and ensure security [16].

Mobile cloud computing is now available in almost all the fields like:

- Mobile learning
- Mobile health care
- Mobile governments
- Mobile commerce
- Mobile banking
- Mobile game

Although mobile cloud computing is spread in every filed but the growing security concerns will slow down the adoption of this technology [17].

[18] says that cloud computing uses' many technologies like operating system, databases, networks, resource scheduling, virtualization, memory management, transaction management, concurrency control and load balancing. As a result the security issues and problems present in all these systems are also present in cloud computing. For instance Security must be kept in mind while mapping virtual machine to physical machine. Securing the data not only involves encrypting the data but also involves using adequate policies during data sharing. All algorithms for managing memory and resources must be secure. Intrusion detection systems use data mining methodologies for finding malware; these can also be used in the cloud for detecting malware.

[19] says that privacy is a major challenge in mobile cloud computing, applications store that data of their users on third party cloud service provider and these third party service providers can sell this data to anyone. Mobile devices can also track locations and they can also provide the location of mobile's owner to any third person. Thus privacy is surely compromised in this way. Mobile devices are most of the time affected with malicious code and thus data can be stolen from mobile. Further they draw our attention to some security related points like data can be leaked from third party applications, vulnerabilities of OS, device can be exploited by hackers, network access can be insecure and unreliable and proximity based hacking can also effect mobile data.

[20] says that mobile cloud computing depends heavily on the network and possible issues that we can face are; bandwidth, delays, non-availability of internet and diversity of hardware and software used. Further once the mobile owner has sent data to the cloud, now the device owner doesn't control the data and he/she has to depend on the cloud service provider for security of his/her data. GPS present in mobile devices has formed the basis for privacy related issues. [21] gave their views that the entire data present on the network must be secured to ensure important information and data are not leaked or hacked. For this purpose strong encryption is necessary. More they say it should be ensured that the entire data going in and out of mobile applications doesn't affect privacy in anyway.

3.0. A HYPOTHETICAL CASE STUDY

Suppose there is a big electricity generating company Electri4500 which is present in country ABC and it has multiple oversea offices. One of the oversea office from country XYZ has done some experiments and they have found an outstanding solution to lower the cost of producing electricity, which can give competitive advantage to Electri4500 over its rival companies. Now the oversea office wants to send data of the new secret design to their main head office in country ABC. They have a mobile app which sends messages and data to the main head office's cloud storage. They don't want any other rival company to get this information or they don't want that any rival company to intercepts the communication between mobile of oversea office and cloud of main head office. In order to protect the data of new design they encrypted the data with a secret key using AES. Now their data is secure they sent the key and data to their head office. The rival company succeeded in intercepting their communication and got both the encrypted data and the secret key. As a result they easily decrypted the design and implemented it before Electri4500 can implement it.

4.0. SOLUTION

The problem shown in the case study can be solved if we encrypt the key. If we want to decrypt something without key we need encrypted text in large quantity so that we can understand and get an idea that how encryption is working. Actually encrypted text in large quantity can help us break encryption but keys are very small and it is very difficult to guess how encryption has been applied on small things like keys. This makes it difficult to decrypt them. We will use Vigenère Cipher to encrypt the key (the key which was being used to encrypt plain text). Vigenère Cipher is based on Caesar cipher but it is stronger as compared to Caesar cipher.

To use Vigenère cipher first of all both parties will have to agree to a key say key_vc which can be anything like code, car, earth etc. Now when both parties have to share some data first of all they will encrypt their data with AES with any key of their choice as they usually do, afterwards they will use Vigenère cipher to encrypt the key with key_vc which they have previously agreed upon.

As Vigenère cipher is based upon Caesar cipher so, let's first explain Caesar cipher and then explain Vigenère cipher. In Caesar cipher we use shifting to encrypt data and similarly we use shifting again to decrypt data. Caesar cipher can be mathematically written as

$$E_i(n) = (n + i) mod 26$$
$$D_i(n) = (n - i) mod 26$$

Here

n = An alphabet from plain text

i = It is a number which tells, that how much increment we need for encryption and similarly it also tells, that how much decrement we need for decryption.

EXAMPLE

Let plain text = mission completed

Let i=3

take n=m from plain text i.e mission completed

$E_3(m)$= m + 3 = p

$E_3(i)$= i + 3 = l

and do the same with all the remaining letters after completion we will get cipher text = plvvlrq frpsohwhg

Lets decrypt now, taking n=l

$D_3(p)$= p – 3 = m

$D_3(l)$= l – 3 = I

And do the same with all the remaining letters after completion we will get back plain text = mission completed

Let's see how Vigenère cipher works.

You know that we will have 2 keys, 1 is for AES let's call it KEY_AES and we have another key for Vigenère cipher let's call it KEY_VC. And surely both parties will decide KEY_VC which both of them will be using to encrypt KEY_AES (both are free to choose anything for KEY_AES)

Suppose both parties decides KEY_VC = sun

Plain text = mission completed

First of all number all alphabet from 0 to 25, see table 1

Table 1 numbering alphabets from 0 to 25

a	0
b	1
c	2
d	3
e	4
f	5
g	6
h	7
i	8
j	9
k	10
l	11
m	12
n	13
o	14
p	15
q	16
r	17
s	18
t	19
u	20
v	21
w	22
x	23
y	24
z	25

After this below each letter of plain text write a letter of KEY_VC and repeat KEY_VC until KEY_AES is not completed as shown in table 2

Table 2 One letter from KEY_VC is placed under each letter of KEY_AES

m	s
i	u
s	n
s	s
i	u
o	n
n	s
c	u
o	n
m	s
p	u
l	n
e	s
t	u
e	n
d	s

"s" has number 18 according to table 1 so, we will shift "m" 18 time and thus replace "m" with "e" and we will continue onwards in the same fashion see table 3 [8]

Table 3 encrypting plain text with Vigenère cipher

m	e
i	c
s	f
s	k
i	c
o	b
n	f
c	w
o	b

m	e
p	j
l	y
e	w
t	n
e	r
d	v

AES stand for Advanced Encryption Standard. It replaced DES back in 2001 on recommendation given by NIST. AES can have key length of 128-bit, 192-bit and 256-bit. On base of the key length the algorithm can be referred as AES-128, AES-192 and AES-256. The data is used in the form of blocks of 4x4 and are called state. For both encryption and decryption AES with 128 bit key will have 10 rounds, AES with 192 bit key will have 12 rounds and AES with 256 bit will have 14 rounds. Each round of AES has the following 4 functions:

1- Substitute byte transformation

An 8 bit substitution box is used to transform each byte of a block into another block.

2- Shift rows transformation

Shifting byte of each row towards left depends on this formula shift=n-1. Where n is the number of row. E.g for n=1 we will have shift=0 so, no byte shift on row 1. Similarly we will have shift=1 for n=2, shift=2 for n=3 and shift=3 for n=4

3- Mix columns transformation

A fixed matrix is chosen and it is multiplied with each column vector. This operation is done in all rounds except the last round

4- Add round key transformation

In this step we do XOR of 128 bit of state with 128 bit of the key.[9,10,11,12,13]

Speed of symmetric cryptographic algorithms is higher for both encryption and decryption, while asymmetric cryptographic algorithms require more time for both encryption and decryption. The asymmetric cryptography have to go through more rounds before data is encrypted or decrypted, as a result they take more time and use more battery power and consumption. We want our communication to be fast and we have limited battery power in mobile thus using symmetric cryptography will be a better solution here

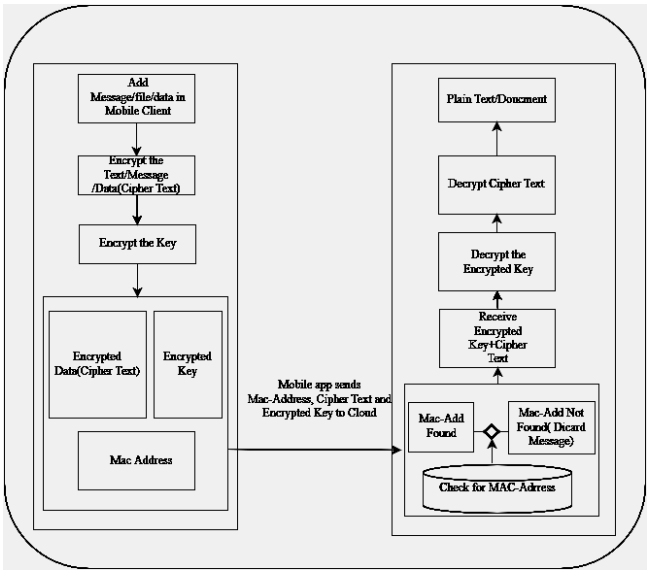

Figure 7: Proposed Solution for a secure Communication in MCC

5.0. SIMULATION

One party wants to upload some data/documents from their mobile to another parties cloud and their app has implemented a security feature similar to described above.

These following steps will be followed for sending cipher text and KEY_AES:

1- Add data/message in mobile app.

2- Enter KEY_AES to encrypt the data/message

3- Enter KEY_VC to encrypt KEY_AES

4- Send data/message from app and KEY_AES from app or from any other source e.g email, mail etc so it remains safe from hackers. (Usually cipher text and key are sent separately for security) (Figure 8)

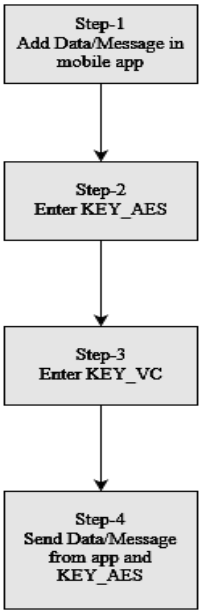

Figure 8: Steps for encryption

These following steps will be followed for decrypting cipher text by using KEY_AES

1- Receive KEY_AES and cipher text
2- Use KEY_VC to decrypt KEY_AES
3- Use KEY_AES to decrypt cipher text (Figure 9)

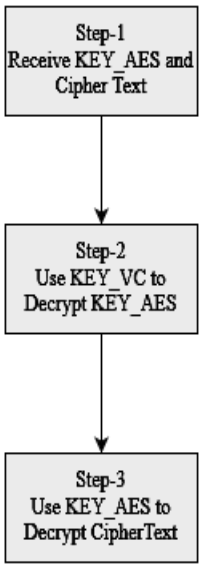

Figure 9: Steps for decryption

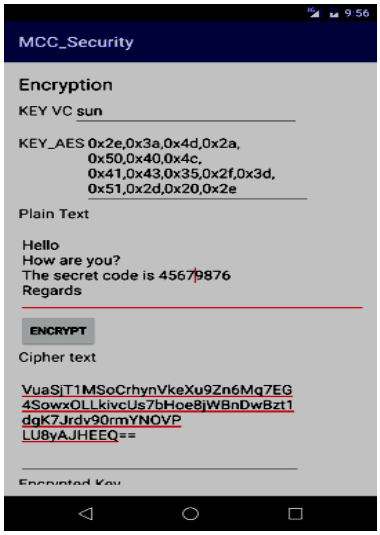

Figure 10.1: Encryption screen of simulation app

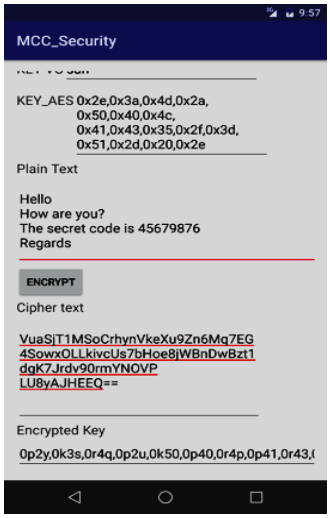

Figure 10.2: Encryption screen of simulation app

Figure 11.1: Decryption screen of simulation app

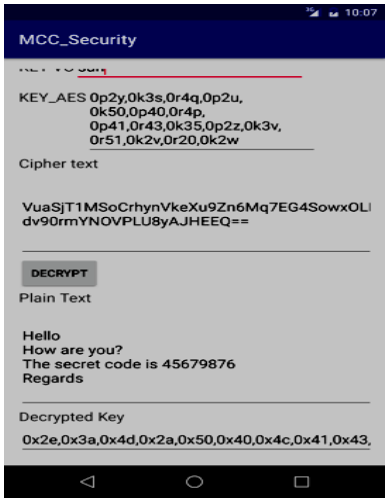

Figure 11.2: Decryption screen of simulation app

Now let's compare the performance of the algorithm with and without Vigenère cipher being used on Key of AES (Figure 12). Left side shows time taken for both encryption and decryption when Vigenère cipher is used and right side shows time taken for both encryption and decryption when Vigenère cipher is not used. Different android devices with different hardware and software configurations will have different performance. This comparison was done using an android virtual device having the following configurations

Name: Nexus_5X_API_23
CPU/ABI: Google APIs Intel Atom (x86_64)
Path: /home/user/.android/avd/Nexus_5X_API_23.avd
Target: google_apis [Google APIs] (API level 23)
Skin: nexus_5x
SD Card:
/home/user/.android/avd/Nexus_5X_API_23.avd/sdcard.img
hw.dPad: no
runtime.network.speed: full
hw.accelerometer: yes
hw.device.name: Nexus 5X
vm.heapSize: 512
hw.device.manufacturer: Google
hw.gps: yes
image.androidVersion.api: 23
hw.audioInput: yes
image.sysdir.1: system-images/android-23/google_apis/x86_64/
tag.id: google_apis
hw.camera.back: none
hw.mainKeys: no
AvdId: Nexus_5X_API_23
hw.camera.front: none
hw.lcd.density: 420
runtime.scalefactor: auto
avd.ini.displayname: Nexus 5X API 23
hw.gpu.mode: auto
hw.device.hash2:
MD5:1be89bc42ec9644d4b77968b23474980
hw.ramSize: 1536
hw.trackBall: no
hw.battery: yes
hw.sdCard: yes
tag.display: Google APIs
runtime.network.latency: none
hw.keyboard: yes
hw.sensors.proximity: yes
disk.dataPartition.size: 800M
hw.sensors.orientation: yes
avd.ini.encoding: UTF-8
hw.gpu.enabled: yes

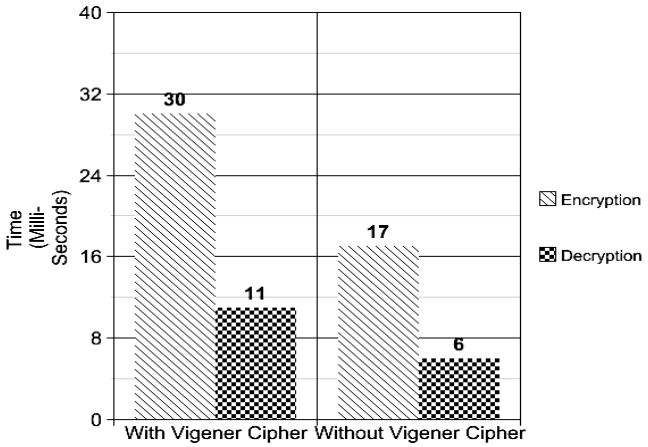

Figure 12: Graph showing the time comparison for doing encryption and decryption with and without Vigenère cipher on the key of AES

6.0. ADDITIONAL SECURITY FEATURE

To make communication more secure we can add mac-authentication on the cloud side. In mac-authentication there will be a list of mac addresses on the cloud. Whenever a client tries to connect with the cloud, client will have to send its mac address to cloud. Cloud will check if that address is present in its list, if it is present then cloud will continue communication with that client. If that mac address is not present then cloud will not communicate with that client.

7.0. RESULTS

As we are using two algorithms to enhance security in mobile cloud computing, thus more time is needed to do it as you can see in the graph (figure 12). As a result of above mentioned solution message/data/document will become more secure as it can be seen in images of mobile showing encryption (figure 10.1, 10.2) and decryption (figure 11.1, 11.2). Our main goal of securing data was successfully achieved.

8.0. FUTURE WORK

In future, work can be done to optimize Vigenère cipher to increase its speed or replacing it with another algorithm which can have more speed with at least same level or higher level of protection offered by Vigenère cipher. Discovering a new algorithm to replace AES which can be more powerful and takes less time for both encryption and decryption. In future we should focus on algorithms which can do efficient and powerful encryption with minimal time requirement.

9.0. CONCLUSIONS

We are living in a society which has started to rely more and more on network and everything from banks to governments are now on the network so, now we can't take the security of the network as optional [14]. Mobiles and other hand held devices are becoming extremely important in our daily lives while on the other hand cloud is becoming very important in the IT world. More and more effort is being put in by IT experts to make each and everything which is used by the public to be made available to them through the cloud.

Meanwhile an adequate effort is also needed to ensure that all the communication between the cloud and the hand held device is protected. Study of different research paper shows that there are multiple loop holes regarding mobile cloud computing which needs to be addressed and fixed. If these are not fixed they can pose a greater threat to the privacy of the general public, national and multinational companies and also to the governments. In this paper an effort has been made to take a step to enhance the security of the communication between mobile and the cloud. The solution proposed here tells that we should take adequate steps to protect our keys which are used to encrypt the data. In this paper we gave a simulation which shows how we can use Vigenère cipher to protect the key used to encrypt the data through AES. Further a graph was presented to show the time comparison when Vigenère cipher is used along with AES and when Vigenère cipher is not used.

Symmetric cryptographic algorithms are both time and resource efficient and we need fast communication with limited resources in mobile cloud computing, thus using symmetric cryptography is better as compared to asymmetric cryptography.

In the end we proposed that mac-authentication can also be applied at the cloud side for additional security. Mac-authentication can ensure that only legitimate clients connect to cloud, get data from cloud and send data to the cloud. We should never leave any system unprotected as the threats today are much more as compared to past.

8.0. ACKNOWLEDGMENT

"This work is supported by National Natural Science Foundation under Grant No. 61163010, the Pre-research Fund of JinChuan Group CO. LTD. under Grant No. JCYY2013012, the Science Project of Lanzhou City under Grant No. 2014-1-171."

REFERENCES

[1]. Hoang T. Dinh, Chonho Lee, Dusit Niyato and Ping Wang, "A survey of mobile cloud computing: architecture, applications, and approaches",*WILEY ONLINE LIBRAY WIRELESS COMMUNICATIONS AND MOBILE COMPUTING*, vol. 13, Issue 18, pp. 1587-1611, 2012

[2]. A. Soomro, M. Lakhan and A. Khan, "THE SECURE DATA STORAGE IN MOBILE CLOUD COMPUTING", *Journal of Information & Communication Technology*, vol. 9, no. 2, pp. 142-150, 2011.

[3]. 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.

[4]. D. Vittapu, D. Sunkari, A. Abate and N. Sreenivas, "A Proposed Solution to Secure MCC Uprising Issue and Challenges in the Domain of Cyber Security", *OPEN JOURNAL OF MOBILE COMPUTING AND CLOUD COMPUTING*, vol. 2, no. 1, pp. 19-33, 2015.

[5]. D. Popa, K. Boudaoud, M. Cremene and M. Borda, "Overview on Mobile Cloud Computing Security Issues", *Seria ELECTRONICĂ şi TELECOMUNICAŢII TRANSACTIONS on ELECTRONICS and COMMUNICATIONS*, 2013.

[6]. "Learn Cryptography - Caesar Cipher", *Learncryptography.com*. [Online]. Available: https://learncryptography.com/classical-encryption/caesar-cipher. [Accessed: 01- Sep- 2016].

[7]. "CrypTool-Online / Ciphers / Vigenère", *Cryptool-online.org*. [Online]. Available: http://www.cryptool-online.org/index.php?option=com_content&view=article&id=51&Itemid=98&lang=en. [Accessed: 01- Sep- 2016].

[8]. B. Veitch, "How to use the Vigenere Cipher", *YouTube*, 2014. [Online]. Available: https://www.youtube.com/watch?v=zNO4PTlg62k. [Accessed: 31- Aug- 2016].

[9]. Mr. Gurjeevan Singh, Mr. Ashwani Singla and Mr. K S Sandha, "Cryptography Algorithm Comparison for Security Enhancement in Wireless Intrusion Detection System", International Journal of Multidisciplinary Research, Vol.1 Issue 4, pp. 143-151, August 2011.

[10]. Akash Kumar Mandal, Chandra Parakash and Mrs. Archana Tiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1-5, 2012.

[11]. G. Singh and S. Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", *International Journal of Computer Applications*, vol. 67, no. 19, pp. 33-38, 2013.

[12]. M. Malhotra and A. Singh, "Study of Various Cryptographic Algorithms", *International Journal of Scientific Engineering and Research*, vol. 1, no. 3, pp. 77-88, 2013.

[13]. J. Chauhan and S. Sharma, "A Comparative Study of Cryptographic Algorithms", *INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD*, vol. 1, no. 2, pp. 24-28, 2015.

[14]. "Cyber risk: Why cyber security is important | White & Case LLP International Law Firm, Global Law Practice", *Whitecase.com*, 2015. [Online]. Available: http://www.whitecase.com/publications/insight/cyber-risk-why-cyber-security-important. [Accessed: 10- Sep- 2016].

[15]. S. Ko, J. Lee and S. Kim, "Mobile cloud computing security considerations", *Journal of Security Engineering*, vol. 9, no. 2, pp. 143-150, 2012.

[16]. A. Bahar, M. Habib and M. Islam, "SECURITY ARCHITECTURE FOR MOBILE CLOUD COMPUTING", *International Journal of Scientific Knowledge*, vol. 3, no. 3, pp. 11-17, 2013.

[17]. M. Sarrab and H. Bourdoucen, "Mobile Cloud Computing: Security Issues and Considerations", *Journal of Advances in Information Technology*, pp. 248-251, 2015

[18]. Innovation Labs, "Security and Privacy Issues in Cloud C loud Computing", Innovation Labs, Tata Consultancy Services Ltd, Kolkata, INDIA.

[19]. A. Donald, S. Arul Oli and L. Arockiam, "Mobile Cloud Security Issues and Challenges: A Perspective", *International Journal of Engineering and Innovative Technology*, vol. 3, no. 1, pp. 401-406, 2013.

[20]. D. Tayade, "Mobile Cloud Computing : Issues, Security,Advantages, Trends", *International Journal of Computer Science and Information Technologies*, vol. 5, no. 5, pp. 6635-6639, 2014.

[21]. P. Kulkarni, D. Khanai and G. Bindagi, "SECURITY FRAMEWORKS FOR MOBILE CLOUD COMPUTING: A SURVEY", *International Conference on Electrical, Electronics, and Optimization Techniques*, 2016.