Journal of Information & Communication Technology
Vol. 9, No. 2, (Fall 2015) 142-150

THE SECURE DATA STORAGE IN MOBILE CLOUD COMPUTING

Amjad Ali Soomro[1],
Mr. Abdullah Raza Lakhan[2],
Department of Computer Science, Mohammad Ali Jinnah University
Adnan Alam Khan[3]
Institute of Business and Technology, Karachi Pakistan

ABSTRACT

Cloud computation is most robust technology of delivering facilities such as software, and hardware (virtual as well) and bandwidth over the internet or network to the customers worldwide. Mobile devices are enabled in order to explore especially, Smartphone. Apple, Google, Face book and Amazon with rich user. Awareness of new security threats and among the customers the mobile cloud computing tell user about new security threats in accessing control data from server. Further it tells security issues can be resolved by proper handling. This paper, will give an awareness regarding cloud computing security issue through encryption and decryption methods when it is explored. If a cloud is performing a task of storage and encryption and decryption of data over the cloud then there can be chance of getting access to the private information without authorization result whole process creates risk of security. I proposed solution regards troubleshooting how to store secure data storage over the cloud with some encryption methods hacker or unauthorized cannot access confidential data owing to encrypted form.

Key Words: cloud computing, security, data security, AES Encryption, Eclipse IDE.

INSPEC Classification : A9555L, A9630, B5270

---

* The material presented by the author does not necessarily portray the viewpoint of the editors and the management of the Institute of Business & Technology (IBT)

1 Amjad Ali Soomro : amjadsoomromscs@gmail.com
2 Mr. Abdullah Raza Lakhan : abdullahlakhan@gmail.com
3 Adnan Alam Khan : write2adnanalamkhan@gmail.com

1. INTRODUCTION

The Cloud Computing is a term it describes utility computing that takes place over the Internet. through internet and vital remote services cloud computing centralize data, applications without physical hardware, paying money and use services of computing by maintaining storage, memory, processing bandwidth etc. All computational resources are visualized and managed automatically through the software.

This study highlighted data handling challenges and related issues regarding private application of user cloud, which is already addressed by many researchers. The paper is organized as follows. Mobile cloud computing defined combining the cloud computing services in ecosystem of mobile that brings the cloud computing and wireless network, which provides wonderful services to the clients [2]. The remote server managed stored user data. So, there are many security issues like modification, data leakage, or data loss [3]. I find out the problem regarding secure data storage over the cloud that when we travel our data to store the cloud provide their security many kinds of attack are possible over the cloud. I provide the mobile encryption and decryption solution.

2. RESEARCH BACKGROUND AND OVERVIEW

The term "cloud" is used as a symbol of the Internet and other communications systems as well as an idea of the underlying infrastructures involved [4].

PAAS is the evolution of the effective virtual computing across the globe in most cheapest and effective way from industry to buyers round the clock. The lack of infrastructure and component knowledge is the most alarming issue address by the end users. Cloud evolution is as follows.

Today necessity or in other words user cannot live without Mobile why because mobile service provides all time connectivity, communication and sharing in most easiest way among humans. The core of mobile technology is mobile applications or App for that enhances the mobile performance with accuracy in fraction of time in most pleasant way. [5]. Today mobile apps are developed not only for communication but also to learn, recreation, and to earn unlike traditional mobile apps such as ringtone editor, grid based games. Technology is advancing at a rapid pace.

2.1 Cloud Computing Service

Cloud computing services these services are broadly divided into 3 major categories: Infrastructure-as-a-Service (IAAS), Platform as a Service(PAAS) and Software as a Service(SAAS).

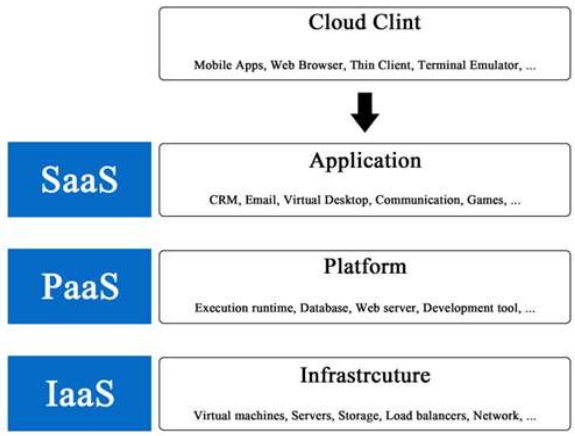

Figure 1: cloud Clint

2.2 Infra-structure as a Service (IAAS)

IAAS usually delivers computing resources to the industry across the globe virtually and efficiently without any physical infrastructure. The prime attraction of cloud services are virtual processing, all time connectivity, proper storage and platform independence. In spite of having physically hardware in their offices placed virtually over IAAS and information is processed over IAAS server on internet. The IAAS provides services like sun to the galaxy like OLX, AMAZON etc.ÊThe main benefit of IAAS is that there is no need to procure computer hardware and its accessories etc [2]. The IAAS services providers have organized data, operating systems and application over rented computing resources [4]. The user can't handle or control the underlying cloud infrastructure but it has have power over operating systems, deployed applications, storage, and maybe limited [11]. The company of IaaS provides off line storage, server and networking hardware as per rent basis and can be access over the cloud [13]. Customer need not to procure the necessary servers, data canter or the network resources. key advantage here is that clients need to pay only for the time period and they can use the cloud service [14].

2.3 Platform as a Service (PAAS)

PAAS mostly provides services of an operating system, further user can run, test their programs. PAAS environment is most suitable for software developers and ERP experts. In PAAS user can easily write, compile and test its own apps or code. The end user site of PAAS cannot administrate underlying cloud infrastructure which includes servers, network, storage or operating systems (O/S) [11].

The paradigm of PAAS mostly deals for delivering operating systems and other services over the internet [13]. Customer uses the required application on PAAS which improves their business wide spread. [14].

2.4 Software as a Service (SAAS)

Software developer uploads their compiled application (app) over SAAS cloud for end user. This compiled software runs over cloud and provides essential services to many end users of multiple organizations. It's a smart contribution to industry by software developer to many clients over SAAS cloud. In contrary now there is no need to run apps on your PC. Further this app can easily be assessed and used by various continents end users clients, apps are easy to use because its thin client [11]. Customization is the main charm of SAAS services providers [2]. SAAS model is famous for it's round the clock service delivery, clients procure, and cloud based apps from service provider [4]. SAAS provider did not support & store client unencrypted data [13]. All apps are monitored and handled by commercial centralized location and its available all across the globe with proper secured network access code [14].

3. RESEARCH METHODOLOGY

This study involves strong literature reviews with different research approaches; initial part is basis of cloud computing and then its services and usage. It also includes research articles of different researchers who have covered data storage techniques and have applied in different areas. Secure data storage by different researchers is also included in this literature study.

Next, few case studies are also referred in this context in which we will try to find the pros and cons of different variations conducted and implemented at various organizations. Such as: AES, DES, RSA and blowfish are famous encryption algorithms which ensure the security of data over cloud. The research will be conducted using Java runtime of Google App Engine, i.e. JDK 1.6 Eclipse IDE. Google 1.6.0 APP Engine SDK or higher Work plan is as follows.

There are multiple pros and cons of mobile based cloud ecosystem, the main issues are linked

with privacy of data, its ownership, content or data Security etc. In contrary advantages are secured cloud accessing, AAA security based cloud access services. Further embedment of identity over mobile device for the sake of protection is possible which can be configure, and personalize on each employee's mobile device, it can also use as personal security token. Corporate based security features and policies are available in this app to enhance maximize security on mobile devices. The following 6 features can provide better security in a cloud of organizations.
We will also refer to the reports published by IEEE, SEI, ACM and other renowned research forums. This method will give us the understanding to implementation of mobile cloud computing as point of security view.

Software and tools: use to implement secure data storage over the cloud.

1. Android SDK
2. Eclipse
3. ADT
4. JAVA
5. SDK+JDK
6. Unit Testing
7. PHP and MySQL

· Literature review for finding the different variations in the mobile cloud computing
· Reports published by IEEE, SEI and other renowned organizations
· Surveys research paper the implementation of secure data storage.

Lastly, we will come up with the programming and model level solution to our problem stated above.

4. EXISTING WORK

We've collected so many reliable research papers from IEEE, Journal of Object Technology and other sources. The literature review of these papers presents many ideas for secure data storage at cloud to meet specific needs. Cloud is initially introduced by Amazon Elastic Compute CloudÊ(EC2).

4.1 DoS Attack

Denial of Service (DoS) is one of most notorious attack by the hacker to hinder cloud services to the end user. The hacker wants to get illegal access to the server, and wants to block cloud services to its legitimate users. Further user did not receive cloud services and find server busy notification which creates unwanted stress, meanwhile the hacker try to get access precious corporate information from cloud servers. DoS attack creates unnecessary anxiety among legitimate users, there are various methods to perform DoS attacks mainly SYN flood. It exploits the transmission control protocol (TCP) in three way handshake by sending connection request to the target server and ignoring the (ACK) acknowledgement from the target server. The hand shaking request is cyclic by the attacker which makes server to respond and waste time and precious resources. Eventually, the target servers tell its legitimate users that cloud services are not available yet please try again later. Cloud administration can prevent these types of attacks by introducing cryptographic based protocols and data encryption standards. In past few years different security agencies has introduced some marvellous technological products which can prevent, detect and filter DoS attack traffic, as you know enterprise security breach rate is dramatically increase in past few years .There is a need to develop more secured cloud based service solutions for its corporate user.

4.2 XML Signature Element Wrapping

Another type of attack is attack via web browser which creates effect on client web services, and also affect cloud computing. Another familiar attack is wrapping of XML signature on web services. Attacker uses XML signature because administration of cloud uses it, i.e., XML signature protects secured fields, element's name, and critical information from unauthorized person, it is not able to protect the information in the document. The attacker is able to control a SOAP message through copying the target element and inserting any value the attacker can insert the original element to everywhere else on the SOAP message. Aforementioned techniques scam the cloud web service by malicious message for attack.

Let say a customer requests a picture called "me.jpg". If the attacker intercept and alters the SOAP message by inserting the same element as the customer but the attackers sent request a document called "CV.docx" in place of the picture. After web service receives the message, the web service will send the CV document back to the customer. E-mail web service application is another type of attack, when hacker intercepts the SOAP message and replaces the e-mail address of a receiver's with an attacker's email address, which result message diversion. Attacks using wrapping XML signature is possible none convey signature information to the referenced element where it is placed. This attack was first introduced by McIntosh and Austel in year 2005 , they have introduced various types of attacks, like Namespace injection , Optional Element in security header, Simple Context, Optional Element etc. These attacks transfers XML document, over the Internet.

4.3 Attack of Malware Injection over Cloud

There is another attack which is called as malware injection over cloud in which it injects malicious code on cloud depending on apps and cloud service. Hacker develops its own app, service or VM and attached to cloud server, then hacker fools the system and shows malicious app as valid instance. Hacker also tries to upload malicious code, virus or Trojan horse over cloud, once the cloud server accepts it as a valid service the malicious code auto run itself and damage the cloud. This virus propagates to another clouds and causes serious damages because most of the clouds using same hardware resources. It's one possible technique which can create a path to damage other cloud or specific cloud. When customer click the app the malicious code run and penetrate from parent cloud to user cloud and infects it precious data. To initiate an attack hacker must compare the service instance image (file type) with the hash value (all new service) so it tricks the cloud and upload the malicious code over cloud. The malicious code is the right word for term malware. This code infected the computer system as well as enterprise network. Whereas Virus is a software auto replicated, self-propagating program which spreads from one system to another system using internet or zombie. Once it infects the PC it infects the system files and start damaging other files and folder. Further it propagates from one source to another.

A Trojan horse is a program that works like a spy, broadcast precious user information to its creator and eventually damages the host system.

4.4 Mobile Terminal Security Issues

Mobile terminal security issues still originated from mobile clients. Firstly mobile customers are usually lacking security awareness; and un-confidentiality; secondly mobile customers may not use themselves properly. So it is needed to find out abnormality of customers owing to troubleshooting above in mobile(MT) terminals, such attacks by hackers may cause information leakage, privacy issues ,disturbance , irregularities and damaged by the hackers over cloud which is deleterious for enterprise and related clients.

4.5 Data Storage Issues

The data stored in a cloud is saving data over an internet or saving data in a virtual world. There are three main types of information security confidentiality, integrity and availability or (CIA). Data encryption is the most reliable solution for data confidentiality. Asynchronous encryption is the best choice in order to achieve two way encryption on user side and server side, it can also encrypt, process, transmit and store large amount of user data on cloud servers in most reliable and efficient way.

5. PROPOSED WORK

5.1 My Model Work

The Model provides full security using JSON - REST API and performing GET, PUT, POST and DELETE (CRUD) operation by JAVA. Java provides the strong encryption method. I applied encryption at JAVA code to plain text and converted it into cipher text. Cipher text is the encrypted file. It's purely secure. And that file sent to cloud server.

6. IMPLEMENTATION OF SECURE DATA STORAGE IN MOBILE CLOUD COMPUTING

The first part contains questions on basic information of security development and its use in different software organizations, its familiarity with the software stakeholders such as software architects, software engineers, software developers, project managers, etc.

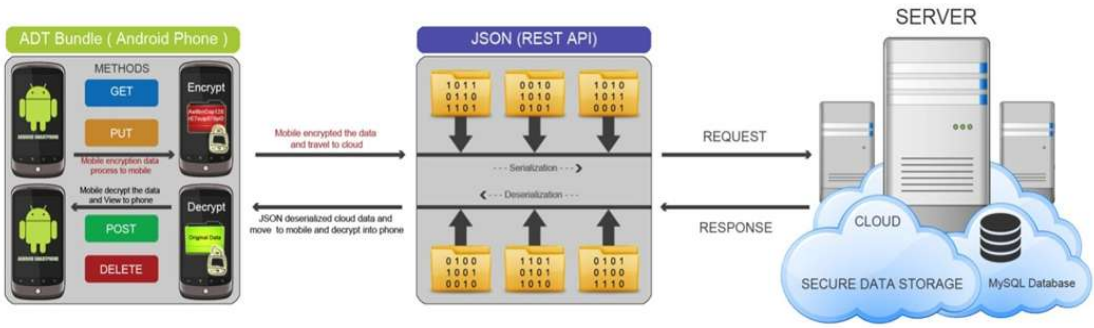

Figure 2: Layout

6.1 Implementation Code

```
Package.com.maju.mcc;

imp0rt. javax.crypto.Cipher;
import.javax.crypto.SecretKey;
import.javax.crypto.spec.SecretKeySpec;

public.class.JEncrytion{

static.String.secretKey = "001234567";

public.static.String.decipher(String_data) throws Exception{
// PKey length= 8
If.(secretKey == null || secretKey.length()!= 8)
```

Figure 3: Frame Work

```
throw new.Exception("Key Invalid! Please enter Eight bytes key ");

Secret.Key.key = new SecretKeySpec(secretKey.getBytes(), "AES");
Cipher.cipher =Cipher.getInstance("DES")
return.new String.(cipher.doFinal(toByte(data)));
        }
Private.static.byte[] toByte(String.hexString)
{
Int.len = hexString.length()./ 2;
byte[].result = new.byte[len];
for (int q = 0;q < len;q++)
result[q]. = Integer.valueOf(hexString.substring(2 *q, 2 *q+ 2), 16).byteValue();
return.result;
        }
Public.static.String.cipher(String_data) throws Exception{
// Eight byte Key length
if (secret_Key == null || secret_Key.length() != 8)
throw new.Exception("Please enter 8 byte key, Invalid!");
SecretKey.key = new.SecretKeySpec(secret_Key.getBytes(), "AES");
Cipher.cipher =Cipher.get_Instance("DES");
cipher.init(Cipher.ENCRYPT_MODE, key);
return.toHex(cipher.do_Final(data.getBytes()));
        }
Public.static.String_toHex(byte[]string_Bytes) {
String_Buffer.result = new_StringBuffer(2 * stringBytes.length);
for (int k = 0; k < string_Bytes.length;k++){
result.apend.(HEX.charAt((string_Bytes[k] >> 4) & 0x0f)).apend(
HEX.charAt(string_Bytes[k] & 0x0f));
                }

Return.result.to_String();
        }
```

```
Private.final static.String _HEX = " ABCDEF 01234506789";
}
```

Aforementioned code explains two way encryption and decryption. Encrypted data provide confidence to legitimate user. IT industry is looking for such type of information encryption algorithm.

7. RESULTS & DISCUSSION

Information portability and availability is the main attraction of IT industry and they are demanding secure channel for their information submission and retrieval. As everyone knows enterprise data is very precious and hackers want to hack enterprise data for sake of money, charm. To overcome this issue our study provides secured encrypted channel which helps organization IT personal, management to save their enterprise data over cloud without fear of hack or loss. The proposed model provides eminent security using JSON - REST API and performing GET, PUT, POST and DELETE (CRUD) operation by JAVA.

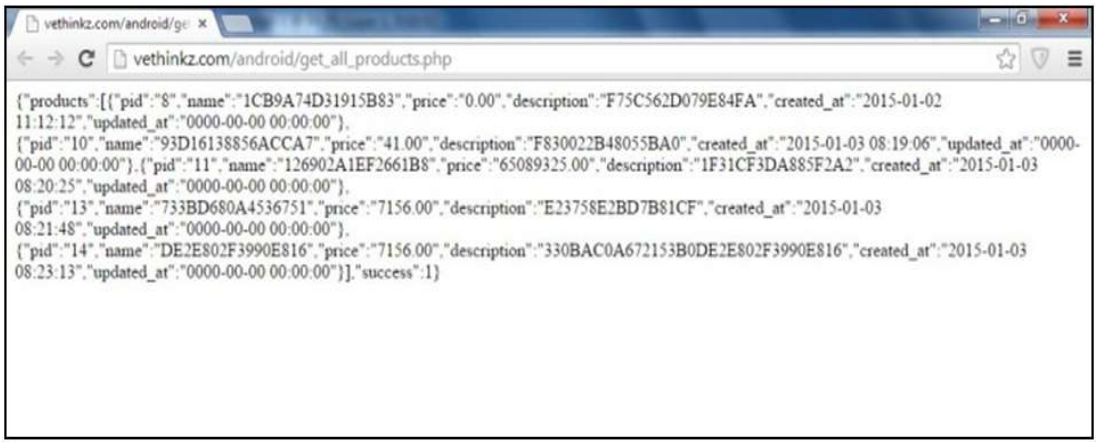

Figure 4: (CRUD) by Java Programming

CONCLUSIONS / FUTURE WORK

In this study we have highlighted a new dimension in the field of information technology which is cloud computing. There are various types of security concerns in cloud computation mainly data authenticity and protection. Further we have developed a smart code which encrypts client data into cipher code on IAAS cloud and ensure clients that their data over cloud is more secured than ever before. We have also addressed hacker's malicious code which propagates in cloud and corrupt end user saved data. This study also provides in-depth solutions to the problem of cloud computation. Today hot topic is cloud for smart phones .This study also answers the unsolved questions of this newly developed field. Mobile computing, cloud computing bridge the enormous gap in the field of communication and technology in recent years. Every technology has some limitation for E.g. enterprise data security issues. This study proposes client data security over cloud. We have developed algorithms to encrypt/decrypt plain text into cipher text over the IAAS cloud where unauthorized user cannot access the client data.

ACKNOWLEDGMENT

First of all with a profound gratitude, we are thankful to Almighty Allah forgiving us success, knowledge and understanding without which we would not been capable of completing this research paper. We are also profoundly grateful to all our family members whose endurance and understanding have played a significant role in our success by sacrificing the important family time and supporting us all over the research work. We are finally thankful to the editor, reviewers and IBT specially who provided us with the opportunity to publish our research paper in this esteemed journal.

REFERENCES

[1] V. Goyal, O. Pandey, A. Sahai, and B. Waters,"Security issues in cloud computing and its Countermeasures ", International Journal of Scientific & Engineering Research, Volume 4, Issue 10, October-(2013),pp.120-1205.

[2] Huang, X. Zhang, M. Kang, and J. Luo. Mobicloud ,"Mobile Cloud Security Issues and Challenges: A Perspective", International Journal of Engineering and Innovative Technology (IJEIT), Volume 3, Issue 1, July (2013),pp.25-28.

[3] D. Boneh, A. Sahai, and B. Waters. ,"DFCloud : A TPM-based Secure Data Access Control Method of Cloud Storage in Mobile Devices ", IEEE 4th International Conference on Cloud Computing Technology and Science (2012),pp. 573–592.

[4] X. Zou, Y.S. Dai, and E. Bertino ,"Cloud Computing Vulnerability: DDoS as its main Security Threat and Analysis of IDS as a Solution Model", 11th International Conference on Information Technology: New Generations ,(2014),PP. 538–546.

[5] D. Boneh, A. Sahai, and B. Waters," Security and Privacy in Mobile Cloud Computing", IEEE Conference,(2006),pp. 573–592.

[6] J. Bethencourt," Countering Wrapping Attack on XML Signature in SOAP Message for Cloud Computing", Proceedings of the 2007 IEEE Symposium on Security and Privacy, (2007),pp.321–334.

[7] E.J. McCluskey. "Mobile Cloud Computing Standard approach to protecting and securing of mobile cloud ecosystems", International Conference on Computer Sciences and Applications, (2013), pp.56-59.

[8] J. Su, J. Scott,"A Survey on Data Security Issues in Cloud Computing: From Single to Multi-Clouds", Journal of Software, VOL. 8, NO. 5, MAY (2013), pp.523-552.

[9] D. Ducamp and H. Schauer, ,"Secure Data Storage for Mobile Data Collection Systems", EEE Conference on Computer Communications ,(2010),pp.58-65.

[10] D. Huang, X. Zhang, M. Kang, and J. Luo, "Security Architecture for Mobile Cloud Computing" -International Journal of Scientific Knowledge Computing and Information Technology , (2012) ,pp.615-619.

[11] J. Su, J. Scott, P. Hui, E. Upton, M. Lim, C. Diot, J. Crowcroft," Management of Security and Privacy Issues of Application Development in Mobile Cloud", Technical Report, UCAM-CL-TR-680, University of Cambridge,(206),pp.612-613.

[12] J. Bethencourt," Environment: A Survey", IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), Jaipur, India, May (2014), pp.92-96.

[13] "Ensuring Distributed Accountability for Data Sharing in the Cloud", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 4, JULY/AUGUST (2012), pp.215-218.

[14] D. Ducamp and H. Schauer "Cloud Computing - Concepts, Architecture and Challenges", International Conference on Computing, Electronics and Electrical Technologies,(2012),pp.502-505.