The Secure Data Storage in Mobile Cloud Computing

Abdullah
Department of Computer Science, Lecturer,Mohammad Ali Jinnah University, Karachi Pakistan
Email: abdullahlakhan@gmail.com

Imran
Department of Computer Science, Lecturer,Mohammad Ali Jinnah University, Karachi Pakistan
Email: imran.ali@jinnah.edu

Fida Hussain
Department of Computer Science, Lecturer,Dawood Engineering University, Karachi Pakistan
Email: fida@gmail.com

Abstract
Cloud computing is a 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, Facebook and Amazon with rich user. The mobile cloud computing technology is growing rapidly among the customers and at the same time it aware us the new security threats. Customers can access their data in any time, at any place, even with any device including mobile devices by using the cloud storage services, although these properties offers flexibility and scalability in controlling data, security issues are overcomes 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.
Keywords:cloud computing, security, data security, AES Encryption, Eclipse IDE.

I. 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.

In this paper, we have highlighted many important of issues and challenges concerning to security as well as privacy in mobile cloud application development work done by several 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.
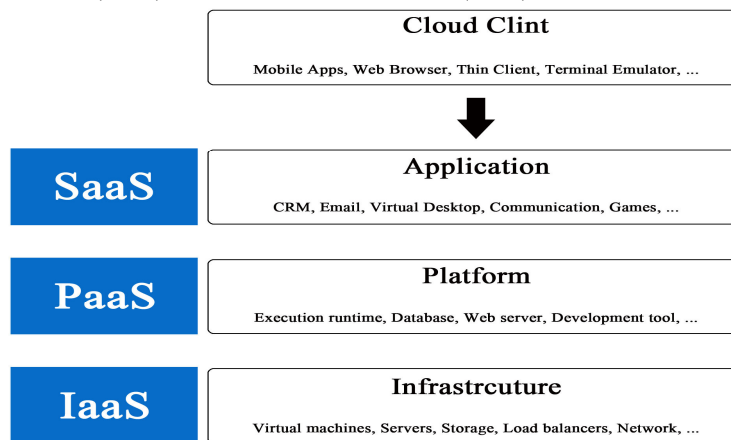
II. Research Background And Overview

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.

What we now commonly refer to as cloud computing is the result of an evolution of the widespread adoption of virtualization, service-oriented architecture, autonomic, and utility computing. Details such as the location of infrastructure or component devices are unknowns to most end-users, who no longer need to thoroughly understand or control the technology infrastructure that supports their computing activities. Following is a brief history of this evolution:

Mobile devices such as Smartphone, Tablets are increasingly becoming an integral part of modern life and culture as the connectivity, communication and sharing has turned out to be easier and convenient among people. Mobile applications (apps) for that matter reduce the performance of task in span of minutes and help deliver accurate results. 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.

A. Cloud Computing Service

Cloud computing services these services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

Cloud Clint

Mobile Apps, Web Browser, Thin Client, Terminal Emulator, ...

SaaS

Application

CRM, Email, Virtual Desktop, Communication, Games, ...

PaaS

Platform

Execution runtime, Database, Web server, Development tool, ...

IaaS

Infrastrcuture

Virtual machines, Servers, Storage, Load balancers, Network, ...

B. Infrastructure as a Service

IaaS mostly offers Utility computing it allows businesses to get infrastructure from providers as virtual resources *as needed* basis. Virtual hardware, raw processors, storage software platforms include computers. In spite of having physically hardware in their offices placed in the 'cloud' and information is accessed through the internet. The basic idea behind IaaS is not new, but this type of cloud computing is getting new life from big providers like Sun, Amazon, Rackspace, IBM, and Google. The main benefit is that there is no need to procure a server or execute physical data center equipment like storage, networking, etc [2]. They have organized over the applications and OSs they install on top of the 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 center 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 [20].

C. Platfotm as a Service

PaaS mostly offers an operating system and providing for software development and testing like suites of programming languages that client can use to develop their own apps. The end user cloud not handle or control the underlying cloud infrastructure including servers, network, storage or operating systems [11]. The paradigm of Paas mostly deals for delivering operating systems and other services over the internet [13]. Application typically required by the customer deployed on it [20].

D. Software as a Service

SaaS mostly offers finished applications on demand for users. Software execute over the cloud and services many end users or client organizations. This is the model of software deployment where an application is hosted as a service provided to customer over the Internet. By eliminating the need to install and execute the application on the customer own computer, The applications are accessible from various customer devices because of a thin client interface such as a web browser (e.g., web enabled e-mail) [11]. This type of service provides complete applications to the clients which is customizable within the confines [2]. SaaS model service delivery, clients procure cloud-based applications from service provider [4]. SaaS provider can't store the unencrypted client data [13]. Network-based access and management of commercially offered software that are handled from centralized locations and enabling clients to access these applications which is remotely over the internet [20].

III. **Research Methodology**

The thesis involves different research approaches; first a literature study is conducted to gain a fundamental understanding of cloud computing and there services and its use in the architectural development of software. 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:

Encryption algorithms like – AES, DES, RSA and blowfish to ensure the security of data in cloud. The research will be conducted using Java runtime of Google App Engine, i.e. JDK 1.6 Eclipse IDE. Google App Engine SDK 1.6.0 or higher. Below are the steps for proposed work plan.

There are many advantages in mobile cloud ecosystem, there are some issues and challenges in mobile

cloud computing. Like: data ownership, privacy and Data Security and other Security Issues.

Possible solution is Cloud-access protection: Strong authentication method ensures that only legitimate user with authorization can access cloud-based services [2]. Embedded device identity protection: It is possible to embed a personalized configuration profile on each employee's mobile device, thereby implementing a credential or personal security token on their mobile device [2]. There are some other security features and policies that can be enforced to maximize the security on mobile devices, especially in a corporate context [2].

Security is an important factor in cloud deployment and by building in the capabilities described in these six steps, organizations can better manage and protect their customer data over the cloud

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.

IV. **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 Cloud (EC2).

DDoS Attack

Denial of Service is such type attacks over the cloud that prevents the clients from receiving the service from the cloud. The attacker are continuously attack to the target server to get the actually clients might not be able to receive the service since the server is busy servicing the attack. There are many techniques to perform DoS attack. Like SYN flood. The SYN flood exploits the TCP 3-way handshake with the help of requesting connections to the target server and ignoring the acknowledgement (ACK) from the server.

Attacker applies attack to the server. This makes the server to wait for the ACK, wasting time and resources.

Eventually, the servers do not have any resources to provide services to the clients. This type of attack can be prevented by authorizing strict access to the cloud and may using cryptographic protocols to make sure that the right personnel are accessing the cloud [1].

There are different technology products have been released to prevent and detect DDoS attacks, the security breach had been growing at a shocking rate both in the cloud computing environments and enterprise.

Xml signature element wrapping

The customers are typically capable to connect to cloud computing via a web browser or web service, web service attacks also affect cloud computing. XML signature element wrapping is the familiar attack for web service. Cloud security uses XML signature to protect an element's name, attributes and value 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. This technique can scam the web service to procedure the malicious message created by the attack.

Because of the figure 3.2, the 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.doc" in place of the picture shown as the figure 3.3. After web service receives the message, the web service will send the cv document back to the customer. Another possible scenario attack may be in the form of the e-mail web service application. When attacker intercepts the SOAP message and changes the receiver's e-mail address to the attacker's email address, then web service will forward the e-mail to the attacker [1].

XML signature wrapping attacks are possible because of the fact that the signature does not convey any information to where the referenced element is placed [13]. This attack was introduced for the first time, in 2005 by McIntosh and Austel [6], stating different kind of this attack, including Simple Context, Optional

Element, Optional Element in security header (sibling value) and Namespace injection (Sibling order) [6]. This attack happens in SOAP message, which transfers the XML document, over the Internet.

Cloud malware injection attack

Cloud malware injection is the attack which tries to inject a malicious service, application over the cloud depending on the cloud service models (SaaS, PaaS and IssA). In order to execute this attack, an intruder is necessary to produce his own malicious application, service or virtual machine instance and then the intruder has to attach it to the cloud system. When malicious software will be added to the cloud system, the attacker has to trick the cloud system to treat with the malicious software as a valid instance. Another scenario is this that may be attacker try to upload a virus or trojan program to the cloud. Once the cloud system treats it as a valid service, if the virus program execute automatically over the cloud infects the virus which can damage to the cloud. Due to this attack virus damages the hardware of the cloud system, other cloud instances running on the same hardware may affect to the virus program because they share the same hardware. Attacker may plan to use a virus program to attack other users on the cloud system. When customer requests the malicious program case, the cloud system sends the virus over to the cloud to the customer and then run on the customer's machine. Client's computer will be impure via the virus. The type of attack could be possible performing a service instance integrity verifying for incoming requests. The hash value may be use to store over the original service instance's image file and compare this value with the hash values of all new service instance images. The result of using the hash values, an attacker is need to create a valid hash value comparison in order to trick the cloud system and inject a malicious instance over the cloud system [1,10].

The term malware refers to any malicious software that could intentionally perform malicious tasks on a computer system or on networked systems. The following covers some basic definitions of the malware problem:

・ **A Virus** is a program that is designed to replicate itself and to spread from one machine to another using an infected (carrier) host program. That is a malicious program copies itself into a program. Once an infected program is executed, the virus starts its functionality, infects and damages the machine. Thus, viruses attempt to spread and infect within the infected machine.

・ **A Trojan horse** is a program that is believed to be useful but which has a harmful intention to wards the host machine. Some hidden part of this type of malware contain a malicious payload that may exploit or damage the host system. Also, Trojan horses can be spyware because of their malicious actions such as the unauthorized collection of a user's data.

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 terminals attacks can cause privacy disturbance leads leakage, irregularity of information and devices damaged by several attacks which is deleterious for clients because of disclose of data to cloud can be hacked [5].
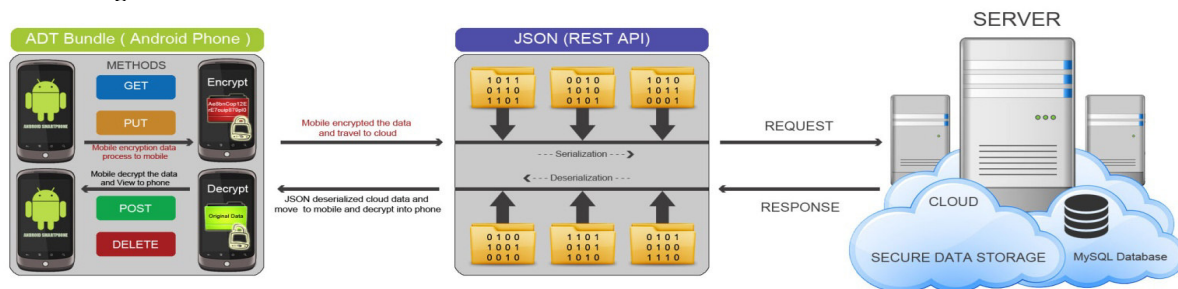
Data Storage Issues

Fig: 4.1 Mobile encryption and decryption proposed model

The data stored in cloud or stored in other places is similar need to consider three different aspects of information security: confidentiality, integrity and availability. The possible solution for data confidentiality is data encryption. In order to ensure encryption there is necessary to consider both encryption algorithm and key strength as cloud computing environment involves large amount of data transmission, storage and handling. Also needs to consider processing time and efficiency of encryption huge amount of data.

V. **Proposed Work**

I proposed work for secure data storage in Mobile cloud computing. I wrote AES (Advanced Encryption Standards) Encryption and Decryption algorithm in Java (JDK and JRE). I have deployed encryption into Amazon Elastic Compute Cloud (EC2). There are three block ciphers consist on AES, AES-128, AES-192 and AES-256. Every cryptographic key using 128-, 192- and 256-bits, listed automatically to encrypt and decrypt data in the blocks. Secrete key or symmetric is using for encryption and decryption. Both sender and receiver

must know while using same secret key. Keep in mind, all key length are enough to protect classified information up to the "Secret" Level with "Top Secret" information. And must require 192- or 256- bit key lengths. There are bits listed below for every round:

1. 10 rounds for 128-bit keys.
2. 12 rounds for 192-bits keys.
3. 14 rounds for 256-bits keys.

Every round consists of many processing steps that include interchange, transposition and mixing of the input plain text and transform it into the final output of cipher text. Cipher text is a text which is not understandable for everyone. Hackers can to also understand it.

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.

VI. 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.

Layout

Implementation

```java
package com.maju.mcc;

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

public class JEncrytion {
    static String secretKey = "01234567";
    public static String decipher(String data) throws Exception {
        // Key has to be of length 8
        if (secretKey == null || secretKey.length() != 8)
            throw new Exception("Invalid key length - 8 bytes key needed!");

        SecretKey key = new SecretKeySpec(secretKey.getBytes(), "AES");
        Cipher cipher = Cipher.getInstance("DES");
        cipher.init(Cipher.DECRYPT_MODE, key);

        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 i = 0; i < len; i++)
            result[i] = Integer.valueOf(hexString.substring(2 * i, 2 * i + 2),
                            16).byteValue();
        return result;
    }

    public static String cipher(String data) throws Exception {
        // Key has to be of length 8
        if (secretKey == null || secretKey.length() != 8)
            throw new Exception("Invalid key length - 8 bytes key needed!");

        SecretKey key = new SecretKeySpec(secretKey.getBytes(), "AES");
        Cipher cipher = Cipher.getInstance("DES");
        cipher.init(Cipher.ENCRYPT_MODE, key);

        return toHex(cipher.doFinal(data.getBytes()));
    }

    public static String toHex(byte[] stringBytes) {
        StringBuffer result = new StringBuffer(2 * stringBytes.length);

        for (int i = 0; i < stringBytes.length; i++) {
            result.append(HEX.charAt((stringBytes[i] >> 4) & 0x0f)).append(
                    HEX.charAt(stringBytes[i] & 0x0f));
        }

        return result.toString();
    }

    private final static String HEX = "0123456789ABCDEF";
}
```
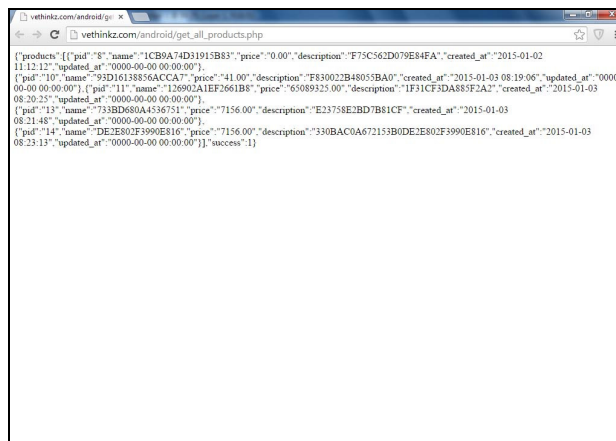
VII. RESULTS

Fig: 6.1 Output from Cloud in the form of Encryption

VIII. Conclusions / Future Work

In this paper I have discussed a new wave in the field of information technology: cloud computing. I have also described its some security issues over the cloud computing. There is no doubt that cloud computing is the development trend for the future. Recently, the mobile cloud computing is becoming a new technology. And the security solution for it has become a research focus. With the development of the mobile cloud computing, new security issues will happen, which needs more security approaches.

I propose research on the data security over the cloud. I used some algorithms to encrypt plain text into cipher text and travel it over the cloud as unauthorized person cannot access it.

References
[1] Security issues in cloud computing and its Countermeasures - *International Journal of Scientific & Engineering Research, Volume 4, Issue 10, October-2013.*
[2] Mobile Cloud Security Issues and Challenges: A Perspective - *International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 1, July 2013.*
[3] 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.*
[4] 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.*
[5] Security and Privacy in Mobile Cloud Computing.
[6] Countering Wrapping Attack on XML Signature in SOAP Message for Cloud Computing.
[7] Mobile Cloud Computing Standard approach to protecting and securing of mobile cloud ecosystems - *International Conference on Computer Sciences and Applications 2013.*
[8] A Survey on Data Security Issues in Cloud Computing: From Single to Multi-Clouds - *JOURNAL OF SOFTWARE, VOL. 8, NO. 5, MAY 2013.*
[9] Secure Data Storage for Mobile Data Collection Systems.
[10] Security in Cloud Computing.
[11] Security Architecture For Mobile Cloud Computing - *International Journal of Scientific Knowledge Computing and Information Technology © 2012- 2013 IJSK & K.A.J. All rights reserved.*
[12] Management of Security and Privacy Issues of Application Development in Mobile Cloud Environment: A Survey - *IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014, Jaipur, India.*

[13]   The Comprehensive Approach for Data Security in Cloud Computing: A Survey - *International Journal of Computer Applications (0975 – 8887) Volume 39– No.18, February 2012.*

[14]   How To Move Your Own Applications Into The Cloud By Exploiting Interfaces Automation And Accessibility Features - *Proceedings of IEEE CCIS2011.*

[15]   Data Security and Privacy Protection Issues in Cloud Computing - *International Conference on Computer Science and Electronics Engineering 2012.*

[16]   Network Security for Virtual Machine in Cloud Computing.

[17]   Dynamic request allocation and scheduling for context aware applications subject to a percentile response time SLA in a distributed cloud- *2nd IEEE International Conference on Cloud Computing Technology and Science.*

[18]   Cloud Computing – Issues, Research and Implementations.

[19]   Ensuring Distributed Accountability for Data Sharing in the Cloud - *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 4, JULY/AUGUST 2012.*

[20]   Cloud Computing - Concepts, Architecture and Challenges -*International Conference on Computing, Electronics and Electrical Technologies [ICCEET] 2012.*

[21]   US-CERT. (2004) Understanding Denial-of-Service Attacks. [Online]. Available: http://www.us-cert.gov/cas/tips/ST04-015.html

[22]   What are the advantages of JSON over XML? [Online]. Available: http://www.quora.com/Markup-Languages/What-are-the-advantages-of-JSON-over-XML.

[23]   Serialization with JSON in Android [Online]. Available: http://android.wanderinghorse.net/2012/06/17/serialization-101-with-json-in-android/.

[24]   Advanced Encryption Standard [online]. Available: http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar