Data Security of Mobile Cloud Computing on Cloud Server

Mohammad Waseem, Abdullah Lakhan, Irfan Ali Jamali

Department of Computer Science and Engineering, Southeast University, Nanjing, China
Email: waseem.sharifkk@gmail.com, Abdullah_raza3@yahoo.com, jamali.irfan@yahoo.com

Received 11 April 2016; accepted 25 April 2016; published 28 April 2016

Abstract

Mobile Cloud computing is a technology of delivering services, such as software, hardware (virtual as well) and bandwidth over the Internet. Mobile devices are enabled in order to explore, especially Smart phones. The mobile cloud computing technology is growing rapidly among the customers and many companies such as Apple, Google, Facebook and Amazon with rich users. Users can access their data at any time, at any place, even with any device including mobile devices by using the cloud storage services, although these properties offer flexibility and scalability in controlling data, however, at the same time it reminds us with new security threats. These security issues can be resolved by proper handling of data. The cloud server provider can secure the data by applying the encryption and decryption techniques while storing the data over the cloud. In this paper, we proposed some encryption and decryption methods for securing the data over the cloud so that an unauthorized person or machine cannot access the confidential data owing to encrypted form.

Keywords

Amazon Cloud Server, Cloud Computing, Security, Data Security, AES Encryption, Eclipse IDE, JSON API

Subject Areas: **Cloud Computing, Information and Communication: Security, Privacy, and Trust, Mobile Computing Systems**

1. Introduction

To have an in-depth understanding of Mobile Cloud Computing (MCC), it is necessary to get a complete grasp on cloud computing [1]. Cloud computing is a new market-oriented business model which offers high quality and low cost information services [2]. Generally, cloud computing resources are provided in the form of services such as Infrastructure as a Service (IaaS), Data storage as a Service (DaaS), Communication as a Service (CaaS), Secu-

How to cite this paper: Waseem, M., Lakhan, A. and Jamali, I.A. (2016) Data Security of Mobile Cloud Computing on Cloud Server. *Open Access Library Journal*, **3**: e2377. http://dx.doi.org/10.4236/oalib.1102377

rity as a Service (SecaaS), Hardware as a Service (HaaS), Software as a Service (SaaS), Business as a Service (BaaS), and Platform as a Service (PaaS). There are various layered architectures available for cloud computing to provide the aforementioned services as a utility [3]. User can consume these services based on SLA (Service Level Agreement) which define their QoS (Quality of Service) parameters on a pay-per-use basis as well as users can access their data any time, at any place, even with any computing device including mobile devices.

Cloud computing with resource constraint mobile devices, ubiquitous wireless infrastructure, mobile web, and location-based services provides a ground for a new computing paradigm called Mobile Cloud Computing (MCC) [4]. The ultimate goal of the MCC is to enable execution of rich mobile applications on a plethora of mobile devices, with a rich user experience [5]. According to the consumer and enterprise market, cloud-based mobile applications are expected to rise to $9.5 billion by 2014. Due to increase in the number of users, there are numerous challenges existing in the field of MCC, including data replication, consistency, limited scalability, unreliability, unreliable availability of cloud resources, portability (due to the lack in cloud provider standard), trust, security and privacy. To attract more potential consumers, the cloud service provider has to target all the security issues to provide a completely secure environment [6]. Many commercial cloud storage services protect user's data stored in server storages by introducing client-based or server-based data encryption.

The objective of this paper is to draw attention to many important issues and challenges concerning with security as well as privacy in mobile cloud application development. This paper also proposes some data encryption and decryption solutions for MCC. The rest of the paper is organized as follows. Section 2 presents the research background and overview. Section 3 researches methodology. Section 4 presents the software and tools and Section 5 concludes the paper with a summary of our contributions.

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.

Cloud computing commonly refers as the result of an evolution of the widespread adoption of virtualization, service-oriented architecture, autonomic, and utility computing. The Details of location of infrastructure or component devices are unknowns to most of the end-users, User doesn't need to thoroughly understand or control the technology infrastructure that supports their computing activities and the users do not necessarily have their own resources. 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 have turned out to be easier and convenient among people. Mobile applications (apps) for that matter reduce the performance of a task in a span of minutes and help deliver accurate results. Today mobile apps are built up not merely for communication, but also to learn, recreation, and to earn unlike traditional mobile apps such as ringtone editor, grid based games etc. Technology is progressing at a speedy rate.

2.1. Cloud Computing Service

Cloud service providers offer their services mainly in three different ways, such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). **Figure 1** describes these three layers of services which are provided by cloud service providers.

2.2. Infrastructure as a Service

IaaS mostly offers Utility computing, which allows users to get infrastructure from cloud service providers as virtual resources as need basis. Virtual hardware, raw processors, storage software platforms include computers.

In spite of having physical 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, according to architecture showing in **Figure 1**, 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. [7]. They have organized over the applications and Operating Systems they install on top of the rented computing resources [8]. The user can't handle or control the underlying cloud infrastructure but it has had power over operating systems, deployed applications, storage, and maybe limited [9]. The company of IaaS

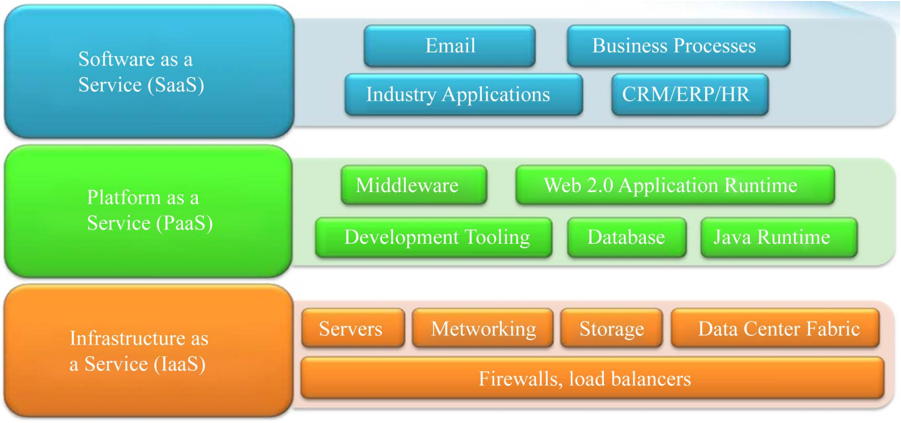


Figure 1. Cloud architecture.

provides off line storage, server and networking hardware as per rental basis and can be accessed over the cloud [10]. The customers need not to procure the necessary servers, data center or the network resources. A key advantage here is that clients need to pay only for the time period and they can use the cloud service [11].

2.3. Software as a Service

SaaS mostly offers executed applications on demand for users. Software executes over the cloud and serve to many end-users or client organizations. This is the model of software deployment where an application is hosted over the Internet and serves to the tenants. This way eliminates the need to install and execute the application on the customer own computer, These applications are accessible from various customer devices because of a thin client interface such as a web browser (e.g., web enabled e-mail). This type of service provides complete applications to the clients which is customizable within the confines [12]. SaaS model service delivery, clients procures cloud-based applications from service providers. A SaaS provider cannot 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.

3. Research Methodology

The paper involves different research approaches; first a literature study is conducted to gain a fundamental understanding of cloud computing and usage of its services 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. Following are the steps for proposed work plan.

There are many advantages in mobile cloud ecosystem. However, there are some issues and challenges in mobile cloud computing such as data ownership, privacy and Data Security and other Security Issues. There are some possible solutions are presented for Cloud-access protection strong authentication method ensures that only legitimate user with authorization can access cloud-based services 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. There are some other security features and policies that can be enforced to maximize the security on mobile devices, especially in a corporate context.

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.

The team will also refer to the reports published by IEEE, SEI, ACM and other renowned research forums. This method will give us the understanding for implementation of mobile cloud computing as point of security view.

4. Software and Tools

Implement secure data storage over the cloud.

A. Android
B. Google API
C. Eclipse
D. JSON
E. JAVA
F. Amazon AWS Cloud server
E. Unit Testing
F. EC2 cloud database

5. Previous Work

According to paper [14], there are many issues in mobile cloud computing due to limitations of mobile devices. Security is the main concern in mobile cloud computing. In Mobile Cloud Computing data of owner is stored on the cloud, which is not secured.

According to paper [15], due to the feature of resource-constrains, security in mobile devices have potential challenges in cloud accessing, consistent accessing, data transmission, and so on. Such challenges can be solved using: special application (service) and middle-ware (provide a platform for all mobile cloud computing systems).

According to paper [15], the security applying on client side of mobile cloud computing are also inherited in mobile cloud computing with the additional limitations of resource constrained mobile devices such as time consuming.

According to paper [16], mobile cloud computing architecture for code offloading in MCC applications, addressing both energy and performance issues due to time constraint.

According to paper [17], all processing in MCC is performed on the mobile side. So there are some issues related to the data travelling such as Bandwidth, latency, availability and heterogeneity.

6. Key components

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 is continuously attack to the target server to get the server busy make a machine or network resource unavailable to its intended users, so that clients might not be able to receive the service from the server, because server will 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 [17].

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.

7. XML Signature Element Wrapping

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.

According to **Figure 2**, customer send data but it is open body. If the attacker intercept and alters the SOAP

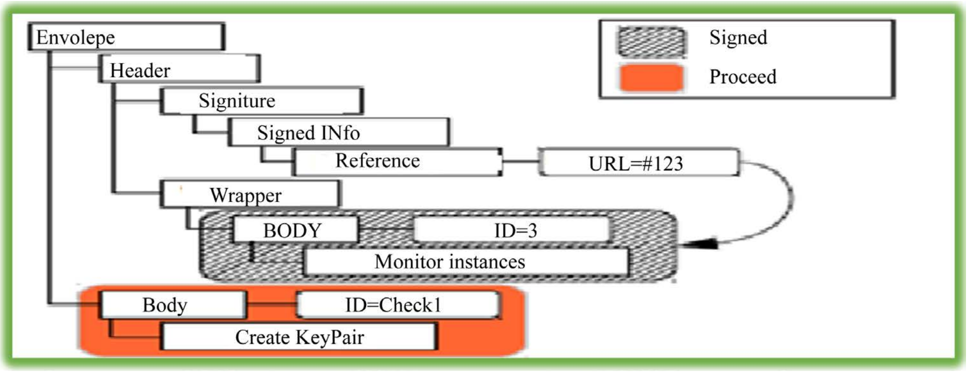


Figure 2. XML data security.

message by inserting the same element as the customer but attackers send request 456 in place of 123. After web service receives the message, web service will send the 456 send back to the customer. Another possible scenario attack may be in the form of e-mail web service application. When the 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.

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. This attack was introduced for the first time, in 2005 by McIntosh and Austel, stating different kinds of this attack, including Simple Context, Optional Element, Optional Element in security header (sibling value) and Namespace injection (Sibling order). This attack happens in SOAP message, which transfers the XML document, over the Internet.

7.1. Malware Attack

Malware attack executes 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 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 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 cloud to the customer and then run on the customer's machine. Client's computer will be impure via virus. The type of attack could be possible, performing a service instance integrity verifying for incoming requests. The hash value may be used 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 needs to create a valid hash value comparison in order to trick the cloud system and inject a malicious instance over the cloud system.

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.

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 copy 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.

7.2. Trojan Horse

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

8. Mobile Terminal Security Issues

Mobile terminal security issues still originated from mobile clients. Firstly, mobile customers are usually lacks 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 terminal attacks can cause privacy disturbance leads leakage, irregularity of information and devices damaged by several attacks which is deleterious for clients because of disclosure of data on cloud can be hacked [17].

9. Related Work

Data Storage Issues

In [17] previous paper according to **Figure 3** discussed about security inside the mobile device before submitting the data on cloud, but we found out the issue about battery consuming, time taking, and because of limited bandwidth some time encryption and decryption performance go down.

According to **Table 1**, 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 by using xml web services. Possible solution for data confidentiality is data encryption. In order to ensure encryption this 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 of huge amount of data.

Cloud is extremely powerful to perform computations while computing ability of mobile devices has a limit so many issues occur to show how to balance the differences between these two. So there are some issues in implementing cloud computing for mobile. These issues can be related to limited resources, related to network, related to security of mobile users and clouds. Some issues are explained as follows.

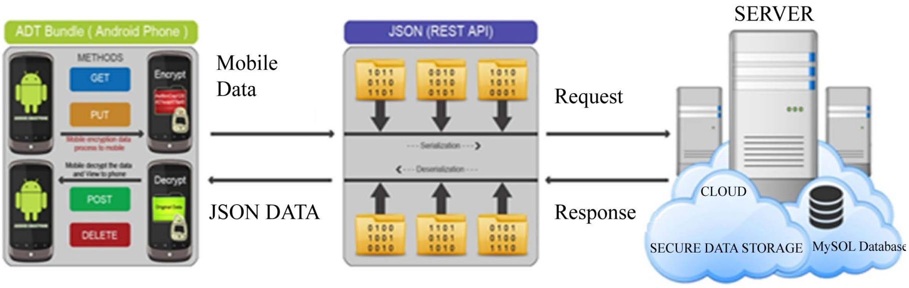


Figure 3. Mobile cloud computing data security.

Table 1. Security Issues in XML.

Issues	Reason
Encryption/Decryption	Time Consuming
Brute Force Attack	Because of open body
Resolve the external entity	Because XML 1.0/1.1 Stand
Implicit trust of internal DTD	Declaring the general entity notation
Configuration catalogs	Entity resolve catalogs
Trust the external schema	External schema definition
UTF-8/UTF-16	Malformed
Sure the trust entity	Import and include construct

10. Proposed Work

According to **Figure 4**, the data of mobile computing travel to cloud computing through JSON object, that is trusted because it has serialize format of data into JSON object, then cloud server will encrypted all data into cryptography, finally it will store in cloud data storage.

According to **Figure 5**, replace the xml web services REST API, and solve the above all problems of "XML", and according to **Figure 5** now data security will be manipulated at cloud server and proposed work for secure data storage in Mobile cloud computing, wrote AES (Advanced Encryption Standards) Encryption and Decryption algorithm in Java (JDK and JRE). Now deploy encryption into Amazon Elastic Compute Cloud (EC2). There are three block ciphers consisted 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. Consider, all key lengths 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

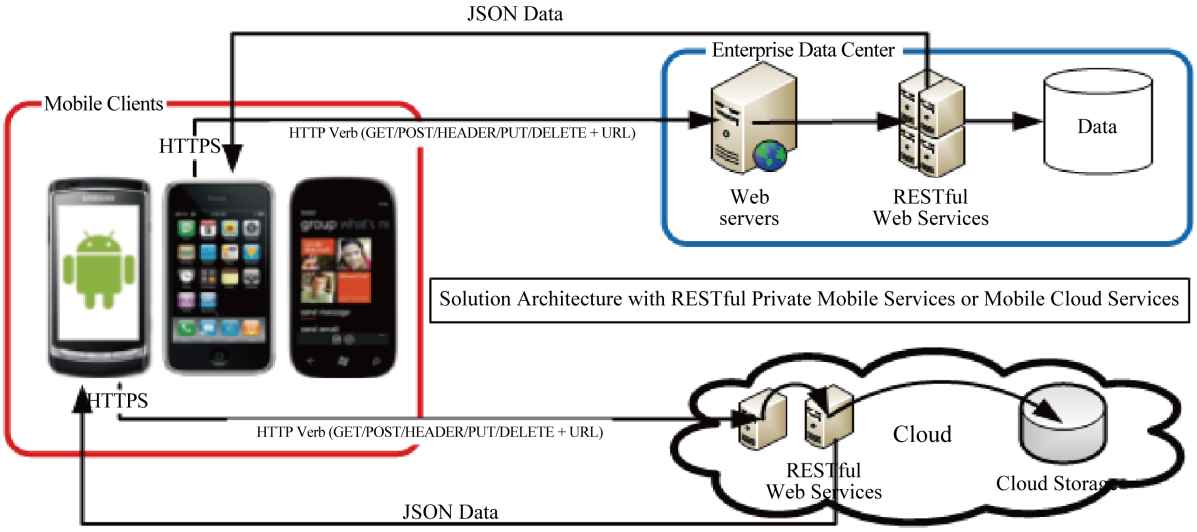

JSON Data
Enterprise Data Center
Mobile Clients
HTTPS
HTTP Verb (GET/POST/HEADER/PUT/DELETE + URL)
Data
Web servers
RESTful Web Services
Solution Architecture with RESTful Private Mobile Services or Mobile Cloud Services
HTTPS
HTTP Verb (GET/POST/HEADER/PUT/DELETE + URL)
Cloud
RESTful Web Services
Cloud Storage
JSON Data

Figure 4. Complete solution mobile cloud computing security on server.

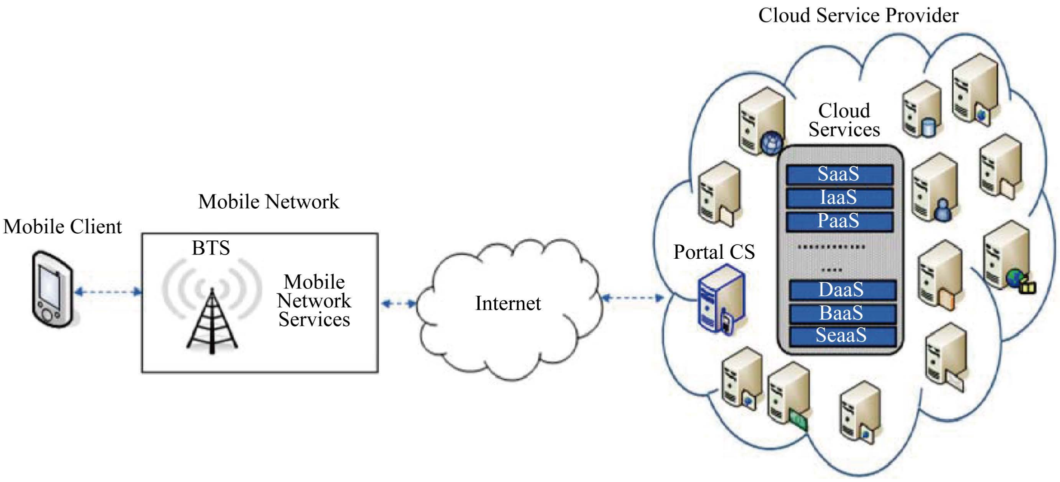


Figure 5. Mobile communication with cloud domain and servers.

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 cannot be understandable by everyone.

10.1. Suggested Research Methodology

According to this research methodology user can manipulate the cloud Amazon services with RESTFUL API integrate cloud service with full security, in our previous work [17] we already mentioned about how to apply security in mobile computing before going to cloud computing, but due to battery consuming and time consuming. This model shows how to overcome the problems by using same methodology and without effect of "QOS".

10.2. Server Side Mathematical Model Encryption Model

A public-key cryptography algorithm which uses prime factorization as the trapdoor one-way function, defines

$$N = pq \tag{1}$$

for p and q primes. Also define a private key d and a public key e such that

$$de = 1\left(\operatorname{mod}\varnothing(n)\right) \tag{2}$$

$$\left(e,\varnothing(n)\right) = 1 \tag{3}$$

where $\varnothing(n)$ is the quotient function; (a,b) denotes the greatest common divisor (so $(a,b)=1$ means that a and b are relatively prime), and $a = b$ mod(a) is a congruence. Let the message be converted to a number M. The sender then makes n and e public and sends

$$E = M^e\left(\operatorname{mod} n\right) \tag{4}$$

To decode, the receiver (who knows ^{d}) computes

$$E^d = \left(M^e\right)^d = M^{e\,d} = M^N\varnothing(n)+1 = M\left(\operatorname{mod} n\right) \tag{5}$$

since ^{N} is an integer. In order to crack the code, ^{d} must be found. But this requires factorization of ^{n} since

$$\varnothing(\varnothing) = (p-1)(q-1) \tag{6}$$

Both p and q should be picked so that $p \pm 1$ and $q \pm 1$ are divisible by large primes, since otherwise the Pollard $p - 1$ factorization method or Williams $p + 1$ factorization method potentially factor ^{n} easily. It is also desirable to have $\varnothing\left(\varnothing(pq)\right)$ large and divisible by large primes.

It is possible to break the cryptosystem by repeated encryption if a unit of $z/\varnothing(n)z$ has small field order (Simmons and Norris 1977, Meijer 1996), where Z/Z^s is the ring of integers between 0 and $^{s-1}$ under addition and multiplication (mod^s). Meijer (1996) shows that "almost" every encryption exponent ^{e} is safe from breaking using repeated encryption for factors of the form

$$P = 2p1+1 \tag{7}$$

$$q = 2q1+1 \tag{8}$$

Whereas another equation joined this equation

$$P = 2p2+1 \tag{9}$$

$$q = 2q2+1 \tag{10}$$

and p, $p1$, $p2$, q, $q1$, and $q2$ are all primes. In this case,

$$\varnothing(n) = 4\,p1\,q1 \tag{11}$$

$$\varnothing\left(\varnothing(n)\right) = 8\,p1\,q1 \tag{12}$$

Meijer (1996) also suggests that $p2$ and $q2$ should be of order 10^{75}.

Using the RSA system, the identity of the sender can be identified as genuine without revealing his private code.

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. We applied encryption in JAVA code to plain text and converted it into cipher text. The cipher text is the encrypted file. It's purely secure. And that file sent to cloud server.

11. Implementation

According to **Figure 5**, the application of cloud is possible in many domains. One of the domains of our current interest is that of mobiles. Hence, we will be focusing on utility of cloud computing environment for mobile usage and how can a cloud add value to the overall functionality and performance of mobile devices? According to [9] as depicted in **Figure 2**, MCC is a service that allows resource constrained mobile users to adaptively adjust processing and storage capabilities by transparently partitioning and offloading the computationally intensive and storage demanding jobs on traditional cloud resources by providing ubiquitous wireless access.

According to **Figure 5**, this architecture is showing the mobile data first step go to private cloud server, which is responsible for data encryption and cryptography. Then encrypted data will go to cloud server that is public and responsible for data storage on cloud database that is EC2 database storage.

The relationship between mobile cloud computing is now secure, the security exist on cloud server that is located privately and safely and public cloud only responsible for storage the encrypted data into data storage. This way user can safely share their important data on cloud server without any hindrance. This concept may be some time taking but very secure for mobile cloud computing.

Authentication and authorization are useful for this architecture, now security flows can occur throw this architecture.

12. Deployed Application

Build an Android app using the IBM Mobile Data for Blue mix cloud service

Store, delete, update, and query objects stored in the cloud

Step-1 Add some grocery list items

Step-2 Restart the application

Notice that your data items have persisted. You now have data on the cloud!

Step-3 See your data on the cloud

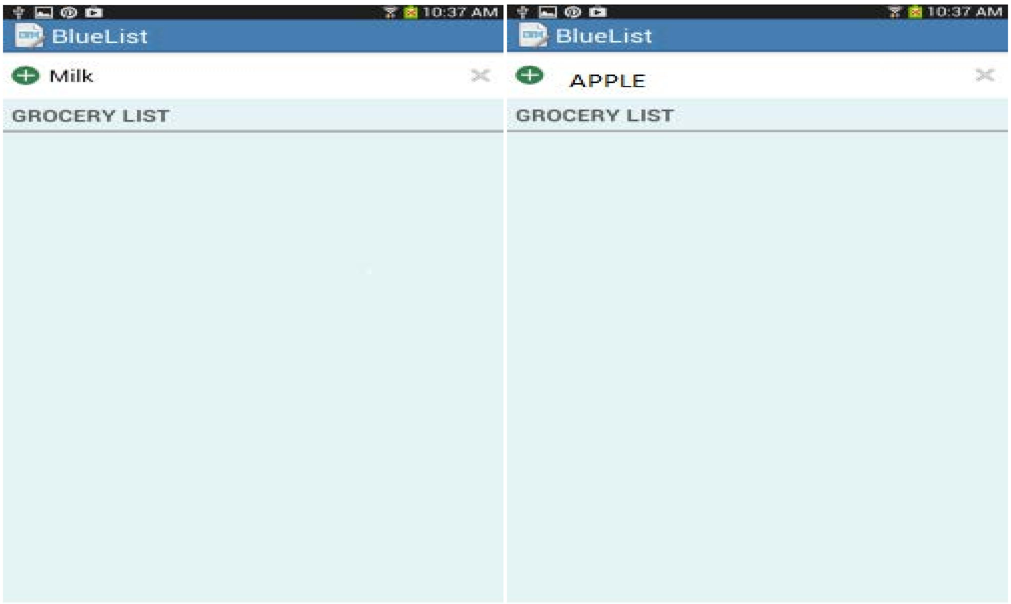
Log in to Blue mix.

Click your application in the Dashboard view.

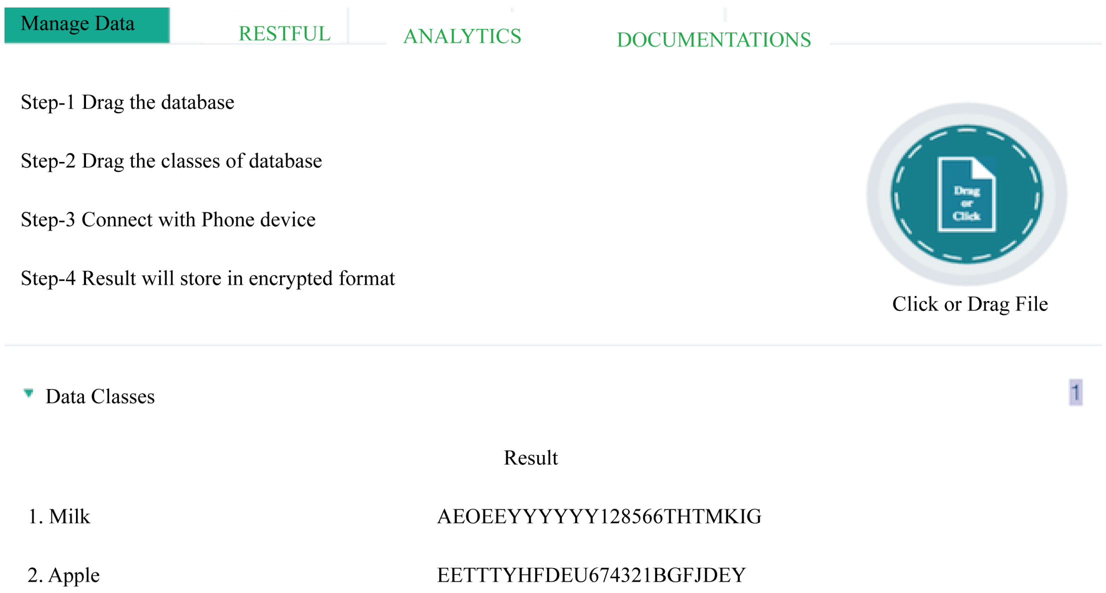
Step-4 On the Manage Data tab, you can see encrypted Data Classes being stored in the cloud, as well as the instances of each Data Class being persisted

Step-5 You can reverse decrypted your data when you again access the data into mobile

Click the Mobile Data Service. Interface for application.



Dashboard



Step-1 Drag the database

Step-2 Drag the classes of database

Step-3 Connect with Phone device

Step-4 Result will store in encrypted format

	Result
1. Milk	AEOEEYYYYYY128566THTMKIG
2. Apple	EETTTYHFDEU674321BGFJDEY

13. Conclusions

The concept of cloud computing provides a great opportunity to users to utilize their services by on-demand basis. The requirement of mobility in cloud computing gave birth to Mobile cloud computing. MCC provides more possibilities for access services in convenient manner. It is expected that after some years a number of mobile users will go to use cloud computing on their mobile devices.

There are many issues in mobile cloud computing due to limitations of mobile devices. Security is the main concern in mobile cloud computing. In Mobile Cloud Computing, data of owner is stored on the cloud, which is not secured.

This paper has provided the description about the basics of Mobile Cloud Computing and issues associated with it. Mainly it discussed about security of data stored in cloud and importance of data security. This paper has explored a number of mechanisms for providing data security so that Mobile Cloud Computing can be widely accepted by a number of users in future. It also proposed a mechanism to provide confidentiality, access control as well as integrity to mobile users.

Acknowledgements

This is the team work, whose help, suggestions, knowledge, experience and encouragement helped to reached research on final results. Team members work hard to try to reduce the problems of client and server side security.

Future Work

In this paper, we present a prototype of the secure data processing model for mobile cloud computing. In the future, we will focus on the follow research: 1) investigate more application scenarios that require data sharing between cloud private domain and public domain; 2) investigate the robustness of the Tri-rooted ESSI solution; and 3) investigate the security monitoring, auditing, and misuse detection in the mobile cloud system.

References

[1] Abrishami, S. and Naghibzadeha, M. (2012) Deadline-Constrained Workflow Scheduling Algorithms for Infrastructure as a Service Clouds.

[2] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee, G., Patterson, D.A., Rabkin, A., Stoica, I. and Zaharia, M. (2013) Above the Clouds: A Berkeley View of Mobile Cloud Computing. Technical Report,

EECS Department University of California, Berkeley. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html

[3] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[4] John, R. (2005) DoD Directive 3020.40, Mobile Cloud Computing Defense Critical Infrastructure Program. 19 Aug, p. 13. http://www.dtic.mil/whs/directives/corres/pdf/302040p.pdf

[5] Ouyang, X.Z. (2011) Cloud Computing in Mobile Communication Networks. Emerging Technologies of Future Multimedia Coding, Analysis and Transmission, No.1. http://wwwen.zte.com.cn/endata/magazine/ztecommunications/2011Year/no3/articles/201110/t20111029_260205.html

[6] Li, X.P., Qian, L.H. and Yang, J. (2015) Workflow Scheduling with Deadline and Time Slots Constraints in Mobile Cloud Computing. *IEEE 19th International Conference on Computer Supported Cooperative Work in Design* (*CSCWD*), Calabria, 6-8 May 2015, 606-613. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7231027

[7] (2011) Adrian Otto's Blog. What Is a Cloud Platform? http://adrianotto.com/2011/02/cloud-platform/

[8] Pooja, N.D. and Ramteke, P.L. (2013) Mobile Cloud Computing. *International Journal of Science and Research*.

[9] Hampton, T.J. (2011) A Quick Guide to Cloud Terminology. 11 August. http://www.thehostingnews.com/a-quick-guide-to-cloud-terminology.html

[10] Lakhan, A. (2015) Security and Data Privacy Using Mobile Cloud Computing.

[11] Rahman, M. and Hassan, R. (2015) Adaptive Workflow Scheduling for Dynamic Grid and Cloud Computing Environment.

[12] Singh, R. (2015) Workflow Scheduling in Cloud Computing Using Spot Instance.

[13] Kaur, N. (2015) Comparison of Workflow Scheduling Algorithms in Cloud Computing.

[14] Kaur, A. (2015) A Review of Workflow Scheduling in Cloud Computing Environment.

[15] Singh, L. and Singh, S. (2015) A Survey of Workflow Scheduling Algorithms and Research Issues.

[16] Lakhan, A. and Hussain, F. (2015) Data Security and Privacy for Cross Platform Using Mobile Cloud Computing.

[17] Lakhan, A.A. (2015) Integration of Dual Data Security Algorithm for Mobile Private Cloud Computing.