Journal of Applied Information Science
7 (2), December 2019, 19-30
http://www.publishingindia.com/jais

Data Encryption Security in Mobile and Cloud Computing Environments

Rashmi P. Sarode[1*] and Subhash Bhalla[2]
[1]The University of Aizu, Japan. Email: d8202102@u-aizu.ac.jp
[2]The University of Aizu, Japan. Email: bhalla@u-aizu.ac.jp
*Corresponding Author

Abstract: The increase in number of smartphones and their applications generates new demands. Smartphones require a higher level of processing power and computation capability. Mobile devices use batteries so their capacity is limited and wireless connectivity also hinders the processing power. Thus, mobile devices being small tend to depend on the server-side support for larger computations and Mobile Cloud Computing (MCC) becomes an emerging field. As mobile cloud computing and its security has become a major hurdle for its adaptability, we discuss the security environment and their issues in mobile cloud computing. We also talk about the diverse and emerging mobile cloud computing applications. Based on an analysis of existing trends, we propose a modified data encryption model for which can secure mobile cloud computing systems and environments efficiently. We conclude the paper by analyzing the advantages as well as limitations of the proposed model and comparing it with related models.

Keywords: Cloud computing, Data encryption, Data security, Mobile cloud computing.

I. Introduction

Cloud computing integrates various technologies to provide platforms, services, and infrastructure to multiple users and business organizations. Mobile Cloud Computing (MCC) combines mobile devices and wireless technologies distributed throughout the environment with cloud computing to enable continuous connectivity. With the rapid advancement of technology, more and more users upload various kinds of data on the cloud, which also includes sensitive data. Data security and privacy are the primary concern when it comes to data sharing [1].

Mobile devices face many privacy issues mainly due to the GPS tracking system. Security of MCC is divided into two main categories – Security module and Privacy module. Security module deals with cloud and mobile network security that can be secured using access control authentication. Privacy module deals with encryption or decryption and sensitive data management [2].

A. Data Security in Cloud Computing

Data security implies that the information will be stored securely, protected from any kind of unauthorized access and also protected from data corruption throughout its lifecycle. This includes data encryption, tokenization, and key management distributions [3].

Organization information is usually shareable, and therefore, data security is compromised. To protect such confidential kind of information, we need data security in MCC systems. If an organization needs a higher level of security and confidentiality, the organization can make a system which is present in multiple servers. Such types of servers are called Mirror Servers.

A cloud storage provider must offer the minimum capabilities which include – a tested encryption schema which the shared storage uses to secure the data, stringent access control protocols so that no unauthorized user can get access to data, data backup has to be scheduled and media backup has to be safely stored [4].

Data need to be protected in three states. The possible states of data are:

(i) *Data in Transit*: Data in transit can be data such as voice, video, text, and metadata. This data moves over the network to cloud and back, so this data has to be encrypted. They involve communication not only with virtual networks but also outside the cloud. They have to be protected against all sorts of attacks by encryption [5].

(ii) *Data at Rest*: This refers to inactive data such as NAS (Network Attached Storage), SAN (Storage Area Network), file servers, data warehouse, and offsite backups. These data should not only be encrypted but

also to prevent attacks, robust access control policies should be used [5].

(iii) *Data in Use*: Data in use refer to dynamic data which are stored in a non-persistent case such as data or encryption keys in the cache, main memory, message transactions in the queue, application data in the process, etc. These data are in clear text form used for searching, retrieval of data. But for better cloud security, these data should be encrypted [5].

Cloud computing often is said to have risks according to analyst firm Gartner [6]. Thus, every cloud provider needs to check the risks on the cloud server in areas such as data integrity, recovery, and privacy. The cloud provider also needs to evaluate the server in legal issues such as e-discovery, regulatory compliance, and auditing [6].

The following security risks arise in cloud computing [6]:

(i) *Privileged User Access*: Leakage of sensitive data will make the data insecure. Data access should be given to a specific set of users.

(ii) *Regulatory Compliance*: Cloud providers have to do external audits and security certifications.

(iii) *Data Location*: Cloud data are located on multiple servers, so the exact location may not be known. They should be asked to follow the local privacy requirements.

(iv) *Data Segregation*: The data in the cloud are stored in shared environments. Cloud providers should help data segregate and should provide evidence of encryption schemes they use because encryption may make any data unusable.

(v) *Recovery*: In case of failure, the cloud provider should be able to restore all data within a short period of time.

(vi) *Investigative Support*: Cloud provider should be able to give investigative support although it is difficult as many users are logging in. Investigation and discovery request would be impossible if the cloud provider is unable to do so.

(vii) *Long-Term Viability*: If the cloud provider loses their business, they should assure you that your data are safe at all costs.

Cloud computing has many challenges in different aspects of data and information handling. Some of these are listed in the following paragraphs [7]:

(i) *Security and Privacy*: Privacy and security problems could be overcome by utilizing secure hardware, encryption security and security applications. Users upload their data on the cloud, and these data are stored randomly on the cloud. Users do not know the specific position of their data being stored on the cloud; this can face a privacy risk.

(ii) *Portability*: This is another obstacle to cloud computing in which software must readily be migrated from one cloud supplier to another. There should be no seller lock-in. However, it is not yet made possible as all cloud suppliers employ different standard languages for their platforms.

(iii) *Computing Performance*: Data-intensive applications on the cloud require high network bandwidth, which results in a high cost. Low bandwidth doesn't meet the desired computing performance of cloud application.

(iv) *Reliability and Availability*: It is vital for cloud technologies to be reliable and robust because the majority of the companies are now becoming reliant on services offered by the third party.

(v) *Interoperability*: This means the application on one platform should be able to integrate services from other platforms. It can be made possible through web services, but creating these web services is quite complicated.

The rest of the manuscript is organized as follows. Section II presents 'Motivation and background'. Section III consists of 'Proposed data encryption security model' and Section IV comprises of 'Summary and conclusions'.

II. Motivation and Background

There are many risks associated with the security of data within the cloud environment, and as MCC essentially uses the cloud, it also inherits any security issues that are associated with cloud computing.

The following risks can arise in a mobile cloud [8]:

(i) *Mobile Terminal*: Mobile terminal has the open operating system having the third-party software, personalization, wireless access internet all the time, so security issues in the mobile terminal are severe.

Malware may be downloaded along with useful programs and may get illegal access to personal user data; thus, mobile terminal will suffer from information leakage. Malware can also enter through a USB device, 3G or 4G networks, Bluetooth or MMS attachments. Though some security vendors provide antivirus software, they should have similar functions to that offered on the desktop. Security issues also arise in application software especially if there is any bug or through the FTP of the application. Bugs can also be present in the Operating System, which can be used to destroy the mobile phone.

(ii) *Mobile Network Security*: Mobile network can be a risk due to public Wi-Fi systems and information can be potentially leaked. Even in the case of Private Wi-Fi, if the encryption mechanism is weak, the network security is at significant risk.

(iii) *Mobile Cloud*: Cloud can also be at risk because of the increase in users sharing information. Attacker maybe a legal cloud user, any inside staff of cloud provider or any of the cloud operator. For example, a 'Denial of Service'

attack will destroy the cloud platform and close all its services.

The basic requirements are to protect and secure data. The cloud service provider needs to design their system in such a way that it protects data from external attacks. Also, the system's architecture and framework should be fault tolerant. In MCC, various factors like confidentiality of mobile cloud-based data sharing exist. The confidential data on a mobile phone are not safe and secure until the Mobile Instrument's Company and the Operating System provide security protocols. Such type of protocols will help to protect our system from external attacks. Besides, the mobile device may be stolen and result in access to highly confidential information [9].

If an organization has to use an MCC environment, the main problem would be to secure the data of the organization. Some of the challenges of MCC are as follows [10]:

(i) *Low Bandwidth*: This is a major issue in MCC that has to be dealt with. As compared to wired network, radio waves provide limited bandwidths which are used in mobile cloud. The bandwidth capacity wavelength that is available is distributed among various mobile devices. Thus, the accessing speed is slow when compared to a wired network.

(ii) *Security and Privacy*: Privacy is also a major challenge in MCC. Threats are difficult to manage in a mobile device as compared to desktop devices, as in a wireless network there are more possibilities of absence of information from the network.

(iii) *Service Availability*: Connection is another kind of major threat in MCC. Mobile users get disconnected. They often complain of transportation crowding, breakdown of network, or becoming out of coverage. Sometimes, mobile users get a signal which has low frequency or low amplitude. This affects the access speed and storage facility.

(iv) *Alteration of Networks*: MCC is used on various operating systems such as Android, Apple iOS, and Windows Phones. Thus, it has to be compatible with all these different kinds of platforms.

(v) *Limited Energy Source*: Mobile devices are usually not so powerful and consume a lot of energy. MCC increases the use of battery of a mobile device which is an important issue related to their design. Mobile devices should have a longer battery life to access all kinds of applications and perform various operations.

To overcome the above problems, a security model must be developed.

A. Related Studies

There are two systems which use the concept of data security in MCC. These are described in the following paragraphs.

FocusDrive- It is a cloud data processing framework through trust management and private data isolation that uses multi-tenancy. The main feature of the cloud service is multi-tenancy. FocusDrive is a pilot mobile cloud system to improve teenagers driving safety. It basically takes care of teenagers who text and drive by restricting the improper usage of a cellphone while driving. It is an application that runs on a mobile phone in the background and monitors the speed of the mobile phone. As per the driving speed and road conditions detected by this application, it enables and disables the texting function in the mobile phone automatically. The public cloud - Microsoft Azure is used as a cloud computing platform in FocusDrive which provides real-time information about the traffic from BingMap API that performs location tracking on a geographic map. To protect user's privacy, it uses the MobiCloud platform as a cloud trusted domain [11].

A virtual machine that is designed for an end user who has full control of the information that is stored in the virtual hard disk is known as Extended Semi-Shadow Images (ESSI). In this framework, each mobile phone is virtualized as an ESSI in the cloud as a trusted domain. ESSI can be represented in a particular application as a service network. On the mobile phone, FocusDrive detects the speedchecker's speed when it reaches a certain threshold which is set by teenager's parent as the application communicates with ESSI in MobiCloud and periodically updates its location via GPS [11].

At the parent's side, they can check the location of their teenager by the service provided by Bing Map and control their teenagers' text function accordingly. The ESSI has a certificate issued by Trusted Authority by which it can select an anonymized identity before sending the location information to the public cloud [11].

Privacy Preserving Cipher Policy Attribute-Based Encryption (PP-CP-ABE) protects the users' encrypted data. Using this, light-weight devices need not disclose data content and security keys while outsourcing encryption and decryption operations to cloud providers. Attribute-Based Data Storage (ABDS) system is a cryptography-based access control system by which information can be achieved by minimizing storage, communication and computation overheads. It also minimizes the costs of cloud which are charged by cloud providers as well as data management costs for communication overheads. Thus PP-CP-ABE is a security data inquiry framework for MCC [12].

B. Mobile Cloud Computing Architecture

MCC uses a computational augmentation approach. With the help of this approach, any resource-constraint mobile device can utilize the computational resources of various cloud-based resources [13].

MCC includes the following four types of resources [13]:

- Distant Immobile Clouds.
- Proximate Immobile Computing Entities.

- Proximate Mobile Computing Entities.
- Hybrid (combination of the above three models).

The general architecture of MCC is shown in Fig. 1. The mobile devices are linked to mobile networks via base stations. Base stations can be base transceiver station, access points or satellites. Base stations establish and control connections such as air links and functional interfaces between mobile devices and networks. Mobile users ask information, and these requests are transmitted to the central processors that are linked to servers providing mobile network services.

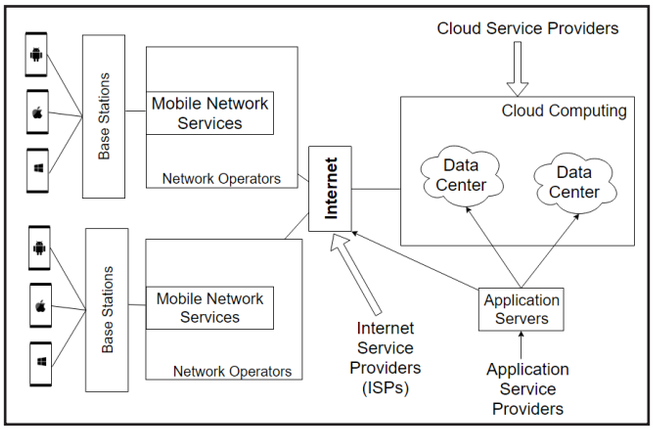

Fig. 1: MCC Architecture

Mobile users are provided services by mobile networks such as authentication, accounting, and authorization based on subscribers and home agent data which are stored in databases. Then, the subscriber's requests are sent to cloud over the internet.

In the cloud, mobile users' requests are processed by the cloud controllers with the respective cloud services. All these services are developed with the concepts of virtualization, utility computing and service-oriented architectures such as application, web and database servers [14].

C. MCC Applications

There are the following applications of Mobile Cloud Computing [15]:

(i) *Mobile Commerce*: Business models for e-commerce can be used via mobile devices using M-commerce. Examples: mobile advertising, mobile financial, and mobile shopping. Mobile commerce applications are confronted with various challenges such as high complexity of devices, low bandwidth, and security. Cloud can be integrated with these applications to address the above issues. For example, to increase the level of security and data processing speed, cloud and 3G services can be combined.

(ii) *Mobile Learning*: The combination of mobility and e-learning is called as Mobile Learning. Traditional Mobile learning has limitations such as high cost of devices or network, limited educational resources and low transmission rate but cloud-based Mobile learning overcomes all these and gives enhanced communication quality between students and teachers. It also helps learns access the remote learning resources and thus helps create a natural learning environment for shared learning.

(iii) *Mobile Healthcare*: Traditional medical treatments have a lot of limitations such as small storage, medical errors, privacy, and security. To overcome these limitations, mobile healthcare has been developed. Mobile healthcare provides mobile users with convenient access to resources such as medical records. It also offers a variety of on-demand services on the clouds to hospitals and healthcare organizations such as health monitoring services, detection of pulse rate, blood pressure, and level of alcohol.

(iv) *Mobile Gaming*: Mobile gaming is the highest potential market for service providers to generate revenues. Mobile gaming can completely offload a game engine which requires a vast computing resource to a server in the cloud which will save energy and increase the game playing time.

(v) *Assistive Technologies*: These are the technologies which provide some kind of assistance such as pedestrian crossing for visually-impaired people, blind people, and transcriptions of lectures for hearing impaired students.

(vi) *Other Applications*: These include monitoring a house, sharing of photos or videos, and smart home systems. The can either be keyword based or voice based.

D. Security Artifacts

There are two major cryptographic algorithms used for the Data Encryption Security Model which are as follows:

1) Advanced Encryption Standard (AES) Algorithm

Triple Data Encryption Standard (TDES) was not considered to be safe against attacks as its significant size is shallow – 56 bits and it can be easily cracked. Thus, a new algorithm AES was needed [16]. AES is also called as Rijndael and is typically used for securing information. To secure data on the cloud, mostly AES algorithm is used. When a user wants to access any application on the mobile cloud, and the user saves the data on the mobile cloud, these data are encrypted by the AES algorithm. When the user wants to access the same data, these are decrypted and sent back to the user [17].

AES is used in banking systems to secure online banking or internet banking, government systems, or high-security systems around the world [18].

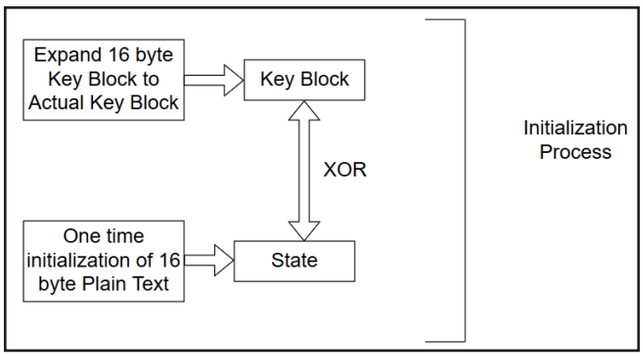

Fig. 2: AES Initialization Process

The main features of AES are as follows [16]:

(i) *Symmetric and Parallel Structure*: This implementation gives the algorithm a lot of flexibility and prevents it against cryptoanalysis attacks.

(ii) *Adapted to Modern Processors*: This algorithm goes well with the modern processors such as Intel Atom, Intel i7, and Pentium.

(iii) *Works Well with Smart Cards*: AES has a block size of 128 bits plain text (4 words/16bytes) and a key size of 128 bits. There are two versions of AES used: 128 bits plain text combined with 128 bits keys size and 128 bits plain text combined with 256 bits key size. (One word = 32 bits). AES has 44 subkeys; each subkey size is 32 bits (1 word/4 bytes). Each round has four subkeys which means 128 bits (4 words/16 bytes) [7].

The first case 128 bits plain text and 128 key size are considered as the commercial standard.

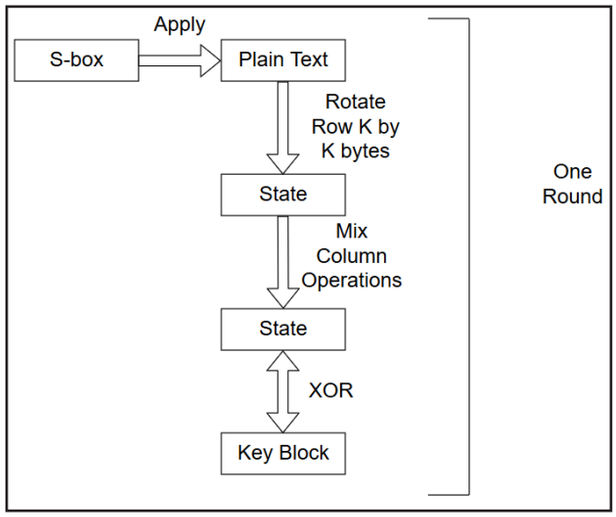

Fig. 3: One Round of AES Process

The AES algorithm can be summarized as follows [16]:

(i) One time initialization process:
  (a) The 16-byte key is expanded to get the actual key block to be used.
  (b) One time initialization of 16-byte plain key text block is done (called as State).
  (c) The state is XORed with the key block.

(ii) There are 10 rounds in AES, for each round:
  (a) S-Box is applied to the plain text bytes.
  (b) Row k of the plain text block (state) is rotated by k bytes.
  (c) A mix column operation is performed.
  (d) The state is XORed with the key block.

Fig(s). 2 and 3 shows the AES initialization and one round of AES process, respectively. For decryption, the process can be executed in the reverse order.

2) RSA Alogrithm

RSA algorithm is an asymmetric algorithm having a key pair for encryption and decryption. The public key is used for encryption which is known to all users as it is published whereas the private key is used for decryption which is only with the respective user.

RSA uses 1024 keys, but 2048 keys are best for security purpose as 1024 keys have 80 bits of symmetric key length which are easy to crack, but 2048 keys are equivalent to 112 bits of symmetric key length which are much more difficult to crack. RSA is used for authentication of the service provider and for the secure communication channel. It is challenging to create a private key from the public key, so RSA is a perfect choice for data encryption [19].

RSA uses the concept of digital signature so that we know the message is not altered in the transit. The number of keys is equal to that of the participants, so this algorithm scales up very well. Also, there is no problem of key exchange in this algorithm [9]. RSA algorithm is used to check that only authorized users can use the application stored on the mobile cloud. If the user saves any message on the mobile cloud, it is encrypted with a public key known to all, but it can be only decrypted with a specific user's private key. The private key is known only to the user who owns the data [10].

RSA is mainly used for digital signatures in different computer applications, commercial satellite radio and satellite TV [9].

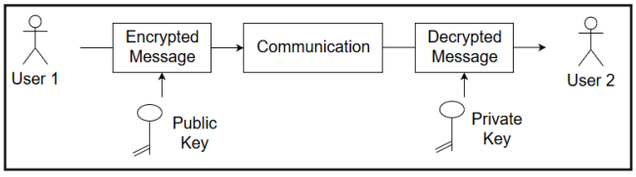

Fig. 4: RSA Algorithm

RSA algorithm is described as follows [17]:

(i) Choose two large prime numbers A and B.

(ii) Choose N in such a way that it is the product of A and B. N = A * B.

(iii) Select encryption key, E, so that is not a factor of (A-1) and (B-1).

(iv) Select decryption key D, so that the following equation is satisfied:

(D*E) mod (A-1) (B-1) = 1

(v) Let the plain text be denoted as PT and cipher text be denoted as CT.

(vi) For encryption, CT = PTE mod N.

(vii) For decryption, PT = CTD mod N.

RSA algorithm is depicted in Fig. 4.

E. QR Code

QR Code (Quick Response Code) was developed in Japan by Denso Corporation in 1994 and later recognized as a standard. [20]. The QR Code is a two-dimensional barcode which has information coded in two directions - horizontal and vertical. Thus, it can store 100 times more data than a barcode [21].

A barcode can contain a maximum of 20 digits whereas a QR code can contain up to 7089 characters. QR code has a special feature that it need not be scanned from a specific angle. QR code scanners are developed in such a way that they can determine the correct way to decode any image as they have three specific squares and alignment blocks in the corner positions of the symbol [22].

QR codes use symmetrical keys which means the same key is used for both encryption and decryption. The key can be created from a sentence or a series of non-meaningful characters. Although QR codes are now used in some of the identification methods such as passports and driving licenses, they are also required in banking, hospitals or healthcare services. It is better to use encrypted QR codes for better security. QR codes are used in a variety of industries like logistics, sales, vehicle manufacturers, telecommunications, and also offline mediums like magazines, newspapers, public transport vehicles, signs, t-shirts, and business cards [23].

QR code has the following characteristics [23]:

(i) All-Direction (360°) High-Speed Reading

The matrix symbols are read using a sensor called as the CCD sensor.

(ii) Resistant to Distorted Symbols

When a QR code is attached to a curved surface or the QR code reader is titled, the symbols get distorted. To correct this QR code has alignment patterns which are arranged in a regular interval within the range of the symbol.

(iii) Data Restoration Functionality

In QR code, the error correction is done in four levels. A code which is arranged in the data area is called the Reed-Solomon code. It is also highly resistant to burst errors.

(iv) Kanji and Kana Characters are Efficiently Coded

QR code is developed in such a way that it can encode Japanese letters as well. A Japanese letter would require 16 bits (2 bytes) for a single character normally; but in QR code, it just needs to be encoded in 13 bits.

(v) Symbols have Linking Functionality

Linking functionality is exhibited by QR codes by which a single symbol can be denoted by many symbols which divide it. Typically, 16 symbols can be formed by dividing a single symbol.

(vi) Code Confidentiality

QR code can be easily encrypted by making a relationship between the unique data stored for special usage and the character type.

F. Cryptography

Cryptology is the science of writing in codes. It comprises of cryptanalysis and cryptography. Cryptography is the science of encrypting information so that unauthorized parties cannot read it and cryptanalysis is the science of decrypting information to understand it without authorization [24].

Thus, cryptography is the art and science of achieving security by encoding messages to make them non-readable. Plain Text is any communication in the language we speak. In other words, a message that can be understood by any person who knows that language. When a plain text is coded by any suitable method, the resulting text is called Cipher Text [17].

Encryption converts plain text to cipher text and Decryption converts cipher text to plain text. There are many algorithms or ciphers to encrypt a plain text so that it gets converted to a cipher text. Each decryption algorithm is associated with a cipher algorithm. Encryption and decryption have a low complexity when a key value is known in an ideal cipher. Though retrieving the plain text without knowing the key or finding the key value has a high complexity. To find the possible keys to decode the message and find the original key, an attacker has to perform a brute force search. An encryption algorithm's security is defined according to the key length [24].

Symmetric key cryptography has the same key to encrypt and decrypt the message. Hence, the problem of key distribution arises.

In asymmetric key cryptography, there is a key pair to encrypt and decrypt the message. The public key is open to all, and private key is the user's personal key.

Cipher text can be generated in two ways: Stream ciphers and Block ciphers.

- *Stream Cipher*: The plain text is encrypted one but at a time.
- *Block Cipher*: The plain text is encrypted by a block of bits in one go [17].

Messages are processed in blocks with the help of Block Ciphers. Each of these blocks are then either encrypted or decrypted with a substitution on huge characters which may be of 64-bits or more. Messages are processed a bit or a byte at the time of encryption or decryption in a Stream Cipher. Most of the current ciphers used nowadays are block ciphers, which are the most widely used types of cryptographic algorithms [14].

G. Mobile Code

Mobile code is a software that is transferred between systems and executed on a local system without being installed on the local system. It can be executed on a single host or many hosts. It can also be transferred from one host to another and can be executed efficiently. It includes scripts like JavaScript, Java Applets, VBScript, Office Macros, DLLs, and ActiveX Controls [25].

There are following advantages of mobile code:

- Eliminate installation and configuration problem and reduce distribution cost.
- Can run many platforms.
- Increase the scalability of client/server applications.
- Achieves performance advantages.
- Achieves interoperability of distributed applications.

There are following properties of mobile code:

- Comes in a variety of forms.
- Often runs unannounced and unbeknownst to the user.
- Runs with the privilege of the user.
- Distributed in executable form.
- Run in multiple threads.
- Can launch other programs.

H. Components in MCC System

Web 4.0 is another term for the Internet of Things, and sometimes it is also called Symbiotic Web. A writer describes this phenomenon as the migration of online functionality to real-world objects. For example, you can run a Google search in your home to find the TV's remote control. This phenomenon of existence is not an enabling technology, but it is a driving technology for MCC [26].

The hypervisor allows the web application to run on any smartphone without being aware of the underlying architecture on it. It also allows other software to run in a virtual environment. Mobile platforms need a built-in hypervisor. For example, the Motorola Atrix has an inbuilt hypervisor which allows a vast number of applications to run on it. It is not necessary that these applications should be built explicitly for the Motorola Atrix [26].

The cloud services are usually defined in a layered concept. In these layers, there are stacks arranged in a particular order. For example, you can have Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) stacked in layers [14, 27].

IaaS is the virtual conveyance of computing resources in the manifestation of hardware, systems administration, and storage administrations. It might likewise incorporate the conveyance of operating systems and virtualization to administer the assets. As opposed to purchasing and instating the needed assets in their own particular server, organizations lease these assets as required [14].

PaaS is a method to rent operating systems, hardware, and network capacity over the Internet. This model allows clients to lease associated services and virtualized servers to run the existing applications or improve or test the new applications [28].

SaaS is a software conveyance strategy that gives access to software and its capacities remotely as a web-based administration. SaaS permits organizations to access business functionality at an expense typically less than paying for authorized applications. Also, because the software is remotely hosted, clients don't have to spend on resources or additional hardware [29].

A mobility-enhanced small cloud data center which is situated on the border of the Internet is known as a cloudlet. The main purpose of cloudlet is to support high resource intensive applications which can be done by providing powerful tools to mobile devices which have lower latency. It's a new component that expands today's cloud infrastructure. It signifies the middle tier of a hierarchy: apparatus - cloudlet - cloud. A cloudlet could be seen as a data center in a box whose objective is to make the cloud closer.

It's been shown that one jump connection from cellular devices to the net isn't efficient. Individuals are sensitive to the present delay in clouds. It appears that latency is not likely to be enhanced. Considering distinct layer for applications like firewall and security, it's improbable that latency improves the growth in bandwidth. This inspires us to utilize cloudlet between mobile devices and cloud pools (Infrastructure) [30].

Virtualization is the ability to run multiple operating systems on a single physical network and share the underlying hardware resources. It is the process by which one computer hosts the appearance of many machines. Virtualization is utilized to enhance IT throughput and prices using physical tools as a pool where virtual resources could be allocated.

A virtual machine (VM) is an isolated runtime environment (guest OS and applications). Multiple virtual systems (VMs) can run on a single physical system.

Cloud and mobile computing take virtualization one step further. There is no need to buy the hardware. Resources can

be rented on the cloud. Various cloud providers allow creating virtual servers. The software and Operating System have to be chosen on the server, and it will run on the server. Many virtual servers can be created on the cloud and can be shut down in minutes.

The same concept can be applied to multi-clouds as well as they avoid dependency on a single cloud. Two or more computing methods such as IaaS, SaaS, or PaaS can be used [30, 27].

III. Proposed Data Encryption Security Model

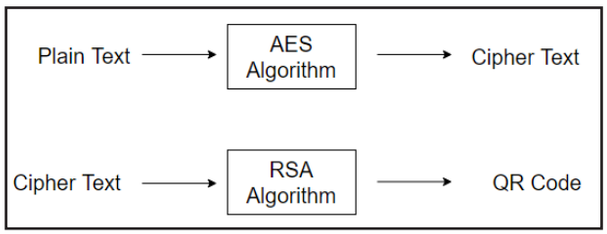

Fig. 5: Encryption Process

We have proposed a security model which can be used by any application to store and secure information as well as validate it. This security model can be used in applications which need online booking or online chat. Similar applications are discussed in the next subsection. The proposed system will first use the AES algorithm and then use the RSA algorithm for encryption and decryption. AES is used in the beginning, as it is faster than RSA in encryption. The end user should not wait for the output to get the QR (Quick Response) Code.

In the encryption process, the plain text will be converted by the AES algorithm to a Cipher Text. The Cipher Text generated by AES algorithm is saved in the database. For security reasons, this Cipher Text is again encrypted by RSA algorithm and then finally converted to QR code which is a lightweight application for mobile devices. Fig. 5 depicts the encryption process.

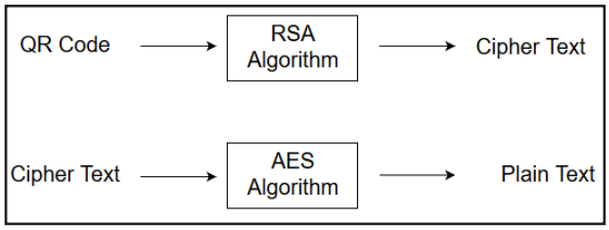

Fig. 6: Decryption Process

Table I: Comparison of AES and RSA W.R.T. Security Elements

Security Elements	RSA	AES
Key Length	2048 bits	265 bits
Iteration Rounds	1	10
Encryption and Decryption Support	Yes	Yes
Application based Web Security Elements	Hardware Tokens Software Tokens Risk-based Authentication On-demand SMS [31]	Hardware Key Passcode Key File System Key File Meta Data File Contents Class Key [32]
Applications	E-banking E-commerce SSL	Transfer Protocols (HTTPS, FTP) Software Applications WiFi Applications (Password Protection)

In the decryption process, QR code will be converted to Cipher Text which will be decrypted by RSA to another Cipher Text which will be saved in the database. This saved Cipher Text will again be decrypted by AES to generate Plain Text. Fig. 6 depicts the Decryption Process.

The reason why we have chosed RSA and AES algorithm for this Proposed Data Encryption Security Model can be understood from the comparison of these two algorithms with respect to their security elements as depicted in Table I.

Demonstration of the Proposed Data Encryption Security Model

Here, we have shown a small demonstration for the proposed model. Fig. 7 shows the encryption process of a plain text to cipher text by AES algorithm. The cipher text gets converted to QR code by RSA encryption.

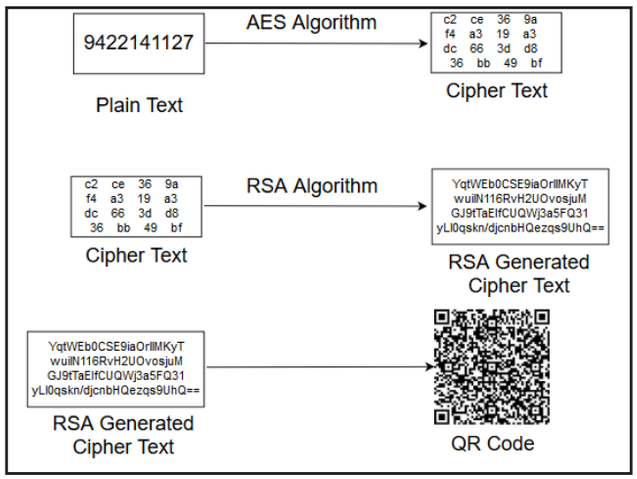

Fig. 7: Demo of Encryption Process

Fig. 8 shows the decryption process. The QR code generated by encryption process is used for decryption. QR code is converted to Cipher text by RSA decryption. The cipher text is then finally converted to Plain text by AES algorithm.

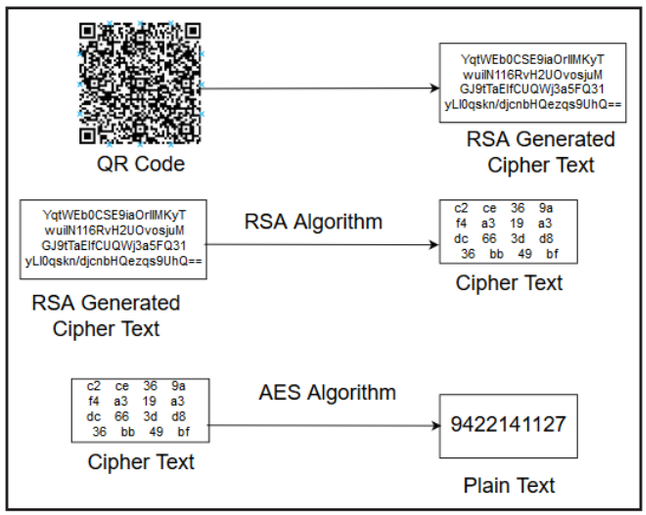

Fig. 8: Demo of Decryption Process

Thus, the output of decryption process gives the same plain text as we had used for the input of encryption process.

A. Existing Applications Similar to That of Proposed System

Consider an application such as BookMyShow which is usually used by users to book Movie Tickets.

BookMyShow is an application that offers movie reviews, movie tickets, movie trailers, events near you, concert tickets, and also gives offers on promotional events and coupons. This application is developed for Indian users. The visitor books a ticket online from BookMyShow and he is sent a QR code on his email. The visitor shows the QR code at the entry of a movie theatre, the official scans his QR Code and only if the QR code is validated, he is granted entry, else he cannot enter the movie theatre. This concept is depicted in Fig. 9.

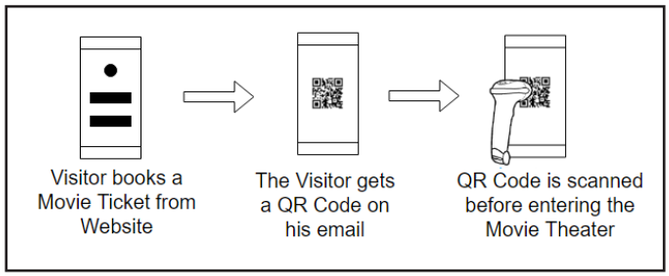

Fig. 9: QR Code Process

The visitor books a ticket and gets a QR code. At the backend, QR code is saved as Cipher Text in the system of the application. Now when the visitor's QR code is scanned at the movie theatre, the scanned QR Code gets converted to Cipher Text and if this Cipher Text matches with that generated at the backend, the Visitor is granted entry. If it does not match, the visitor is not permitted to enter the movie theatre. This concept is explained in Fig. 10.

Consider another application - IRCTC (Indian Railway Catering and Tourism Corporation) which is using a similar concept. IRCTC is the subsidiary of Indian Railways which handles the online ticketing, catering, and tourism operations of Indian Railways. When a ticket is booked through IRCTC in a proper manner, it consists of a QR code which is similar to that in BookMyShow. Thus, the validation of IRCTC QR code is done with a specialized application that is developed by IRCTC.

Consider yet another application - Paytm. Paytm is an e-commerce payment system and also a digital wallet company. Paytm is an application developed for users in India. When we want to make any kind of payment with the help of Paytm, we can do it with a user's Paytm QR code and upon scanning that QR code, we can directly pay to that particular user.

B. Advantages of the Proposed Algorithm

There are the following advantages of the proposed algorithm:

- The proposed algorithm involves two major security protocols namely, AES and RSA. These algorithms have very secure mechanism; thus, the possibility of brute force attack is less.

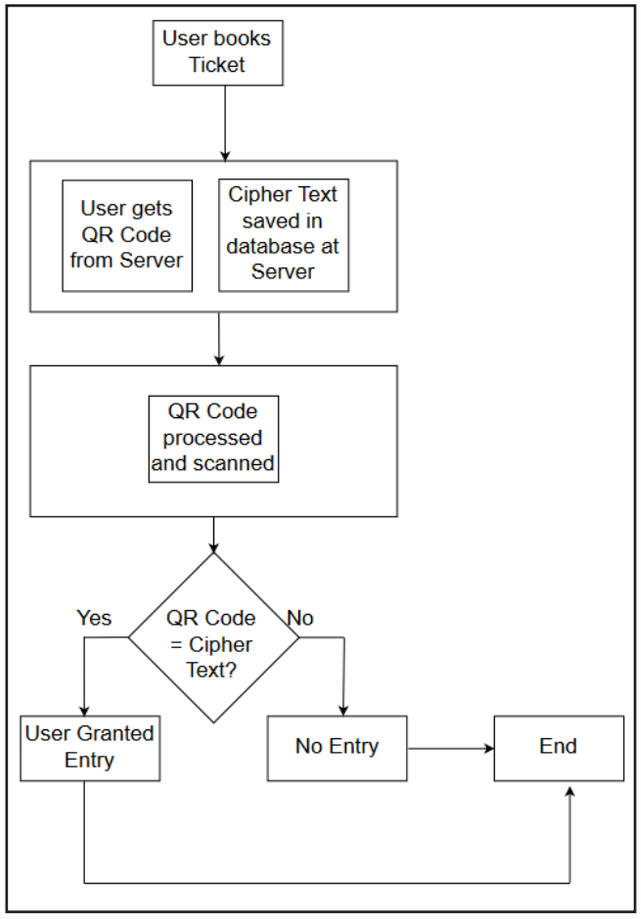

Fig. 10: QR Code Validation

- Normally, algorithms have only Cipher Text involved in their encryption and decryption process; but here, the proposed algorithm uses QR code with Cipher text which makes this algorithm secure.
- The proposed algorithm works on a real-time basis, the keys namely, public key and private key are automatically taken care due to the involvement of RSA algorithm. Thus, key distribution problem is solved here.
- Cyclic Redundancy Check (CRC) mechanism ensures that there is no duplicate entry. In the proposed algorithm, we have a unique QR Code generated for every encryption and decryption process; thus, the concept of CRC is well utilized in this algorithm.
- As QR codes can be accessed by any mobile or handheld devices, the usage of paper is eliminated by the proposed algorithm.

C. Limitations of the Proposed Algorithm

A small amount of data can be stored in QR code. Therefore, we have converted it to cipher text which will ensure that data are secure and these are easy to access the QR code. In this way, one not only needs a smartphone but also an internet connection.

D. Comparison with Other Frameworks

FocusDrive [11] - In the multi-tenancy decentralized approach, there are two security levels – critical data and normal data. A key generated by the user can secure critical data and a key generated by the cloud service provider can secure normal data. The data operations and security operations are distributed to the ESSIs so that the computation overhead is processed on multiple processors in the cloud system. The ESSIs enhance the user's security by adding one additional layer of security in which critical data is stored in ESSI [11].

The proposed new secure data processing mobile cloud infrastructure is depicted in Fig. 11. The mobile cloud basically compromises of three domains – cloud mobile and sensing domain, cloud trusted domain and cloud public service and storage domain. In this model, in the cloud trusted domain, every mobile device is virtualized as an ESSI which can be represented as a Service Node (SN) in a particular application (Service Domain). In a mobile device, the ESSIs can address computation deficiencies and communication. They also provide enhanced security and privacy protection. According to the capability, a mobile device and its ESSI can act as a service provider. This kind of approach will utilize the maximum advantage of a mobile node using cloud computing technologies. In this way, cloud's boundary is extended to customer device domain. The networking between ESSI and the user is through a secure connection such as SSL or IPSec [11].

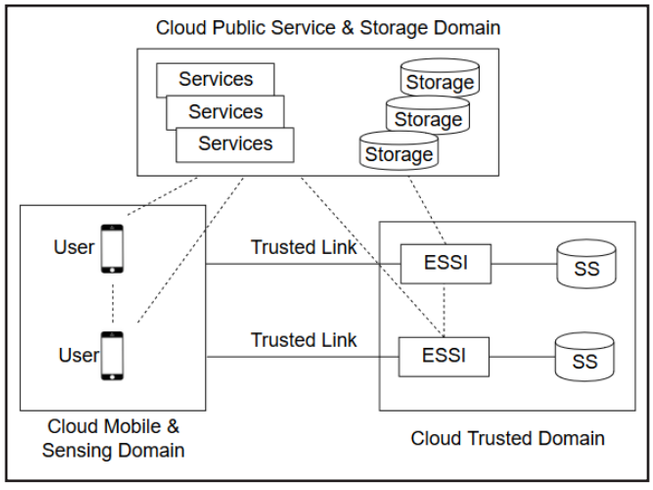

Fig. 11: Reference Service Model of Mobile Cloud [11]

Our proposed solution consists of two algorithms which are very secure as it acts like two-factor authentication. Usually, OTP (One Time Password) is needed in two-factor authentication but here QR Code acts like OTP as QR code will be unique for every mobile. No one will know which QR code will be delivered to which mobile device, so QR code acts like second-

factor authentication security. Cipher text can validate QR code authenticity.

In the proposed framework for PP-CP-ABE services as shown in Fig. 12, before sending the data to the storage service provider (SSP), the data should be encrypted. The encryption service provider (ESP) will provide an encryption service to the data owner in such a way that the provider will not know the encryption key. The Decryption Service Provider (DSP) without knowing the content of data will provide decryption service to the data inquirers. Even if SSP, ESP, and DSP cooperate in some manner, the data content will not be revealed. As shown in the Fig. 12, the proposed system is formed by the three components: SSP, ESP, and DSP. A Data Receiver (DR) inquires data which are provided by Data Owner (DO). Privacy Preserving Cipher Policy Attribute-Based Encryption (PP-CP-ABE) services are provided by ESP and DSP and storage services are provided by SSP. A semi-trusted cloud provides data security in addition with computing and storage services [12].

In PP-CP-ABE, the private key is blinded and the expensive pairing operations are outsourced to the Decryption Service Providers to overcome the high computation issues. The original private key need not be disclosed anywhere, thus user's privacy is not at risk [12].

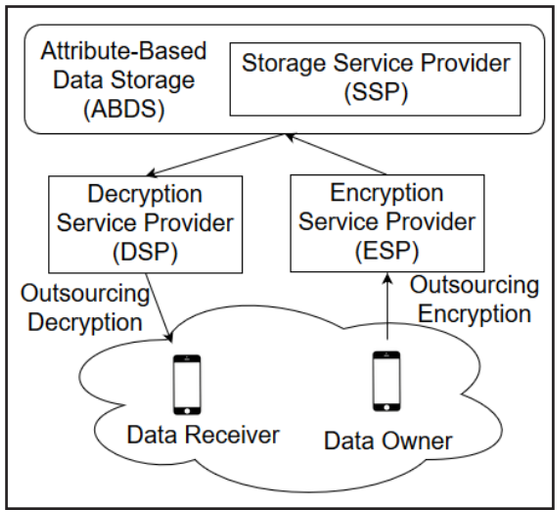

Fig. 12: PP-CP-ABE Framework [12]

In our proposed solution, QR codes are generated which are not easy to break, thus providing a better security solution. RSA algorithm uses a private key and every private key is user specific and it need not be disclosed anywhere.

QR code makes it easier to read the actual information of the user in a very secure manner by the technical team that scans the QR code in real time. Thus, the QR code gives an extra layer of security as user information can be directly accessed in terms of plain text. The information QR code contains needs some specialized hardware and software to read, which is the main bridge between the user and the technical team to analyze the user authenticity.

IV. Summary and Conclusions

There are a number of issues regarding security management in mobile and cloud computing. In the current scenario, various errors and bugs are encountered daily. These may contradict the security protocols. To overcome this issue, we have integrated AES Algorithm, RSA Algorithm, along with QR code in this study to propose a data encryption model for the security of MCC. The architecture of MCC and its components as well as services have been presented with a modified perspective. Existing applications similar to that of proposed system have been explained with figures. The proposed study is compared with two existing frameworks - FocusDrive and PP-CP-ABE.

A secure data encryption model is proposed that helps in securing data in the mobile cloud. To enhance the security of the proposed model, we have used two cryptographic algorithms instead of one and we have also used QR code as a lightweight application becomes easier to access for mobile users. This system consists of cloud framework with APIs. Thus, this system can be integrated with other cloud-based frameworks.

References

[1] Y. Zhang, X. Chen, J. Li, D. S. Wong, H. Li, and I. You, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing," *Information Sciences*, vol. 379, pp. 42-61, 2017.

[2] P. A. Aware, V. Shinde, and A. Aware. "Security issues in mobile cloud computing," *International Journal of Innovations in Engineering and Technology*, vol. 6, no. 1, pp. 105-110, October 2015.

[3] Data Security. Available: https://www.microfocus.com/en-us/what-is/data-security

[4] L. M. Kaufman, "Data security in the world of cloud computing," *IEEE Security and Privacy*, vol. 7, no. 4, pp. 61-64, 2009.

[5] T. Bhatia, and A. K. Verma, "Data security in mobile cloud computing paradigm: A survey, taxonomy and open research issues," *The Journal of Supercomputing*, vol. 73, no. 6, pp. 2558-2631, 2017.

[6] https://www.infoworld.com/article/2652198/security/gartner--seven-cloud-computing-security-risks.html

[7] Cloud Computing Challenges. Available: https://www.tutorialspoint.com/cloud_computing/pdf/cloud_computing_challenges.pdf

[8] U. Somani, K. Lakhani, and M. Mundra, "Implementing digital signature with RSA encryption algorithm to enhance the data security of cloud in cloud computing," *2010 1st Int. Conf. on Parallel, Distributed and Grid Computing (PDGC 2010)*, IEEE, 2010.

[9] S. Gupta, and P. Gupta, "A study of the issues and security of cloud computing," *International Journal of Computer Science and Information Technologies*, vol. 5, no. 4, pp. 5429-5434, 2014.

[10] https://aboutdigitalcertificate.wordpress.com/2014/03/10/5-top-challenges-in-mobile-cloud-computing-2/

[11] D. Huang, Z. Zhou, L. Xu, T. Xing, and Y. Zhong, "Secure data processing framework for mobile cloud computing," *2011 IEEE Conf. on Computer Communications Workshops (INFOCOM WKSHPS),* IEEE, 2011.

[12] Z. Zhou, and D. Huang, "Efficient and secure data storage operations for mobile cloud computing," *Proc. of the 8th Int. Conf. on Network and Service Management*, International Federation for Information Processing, 2012.

[13] Mobile Cloud Computing. Available: http://www.moycom.de/english/strategies-solutions/mobile-cloud-computing-mcc/

[14] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," *Wireless Communications and Mobile Computing*, vol. 13, no. 18, pp. 1587-1611, 2013.

[15] G. Mastorakis, C. X. Mavromoustakis, and E. Pallis, *Resource Management of Mobile Cloud Computing Networks and Environments*, IGI Global, 2015.

[16] A. Kahate, *Cryptography and Network Security*, Tata McGraw-Hill Education, 2013.

[17] R. Arora, and A. Parashar, "Secure user data in cloud computing using encryption algorithms," *International Journal of Engineering Research and Applications*, vol. 3, no. 4, pp. 1922-1926, 2013.

[18] H. Suo, Z. Liu, J. Wan, and K. Zhou, "Security and privacy in mobile cloud computing," *2013 9th Int. Wireless Communications and Mobile Computing Conference (IWCMC)*, IEEE, 2013.

[19] R. P. Sarode, P. Gupta, and N. Manglani, "A comparative analysis of RSA and MD5 algorithms," *Journal of Computer Science and Applications*, vol. 6, no. 1, pp. 25-33, 2014.

[20] Y. Liu, J. Yang, and M. Liu, "Recognition of QR Code with mobile phones," *2008 Chinese Control and Decision Conference*, IEEE, 2008.

[21] P. Kieseberg, M. Leithner, M. Mulazzani, L. Munroe, S. Schrittwieser, M. Sinha, and E. Weippl, "QR code security," *Proceedings of the 8th Int. Conf. on Advances in Mobile Computing and Multimedia*, pp. 430-435, ACM, 2010.

[22] Encrypted QR Codes. Available: https://qrworld.wordpress.com/2011/11/27/encrypted-qr-codes/

[23] QR Codes. Available: https://foxdesignsstudio.com/uploads/pdf/Three_QR_Code.pdf

[24] R. R. Brooks, *Disruptive Security Technologies with Mobile Code and Peer-to-Peer Networks*. CRC Press, 2004.

[25] Internet Security and Firewalls. Available: http://www.gksahu.com/assets/resource/UNIT_4.pdf

[26] Mobile Cloud Computing. Available: https://www.ibm.com/developerworks/cloud/library/cl-mobilecloudcomputing/index.html

[27] R. G. Patidar, and S. Bhalla, "Recent developments in mobile cloud computing," *Journal of Emerging Technologies and Innovative Research*, vol. 6, no. 2, pp. 46-51, 2019.

[28] C. V. Raja, K. Chitra, and M. Jonafark, "A survey on mobile cloud computing," *International Journal of Scientific Research in Computer Science*, *Engineering and Information Technology*, vol. 3, no. 3, pp. 2096-2100, March-April 2018.

[29] S. Alonso-Monsalve, F. García-Carballeira, and A. Calderón, "A heterogeneous mobile cloud computing model for hybrid clouds," *Future Generation Computer Systems,* vol. 87, pp. 651-666, 2018.

[30] Cloudlet. Available: https://searchcloudcomputing.techtarget.com/definition/cloudlet

[31] RSA SECURID. Available: https://www.rsa.com/content/dam/en/data-sheet/rsa-securid-management-console.pdf

[32] iOS Security. Available: https://www.apple.com/business/docs/site/iOS_Security_Guide.pdf