Journal of Information Security, 2016, 7, 245-259
Published Online July 2016 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2016.74020

Scientific Research Publishing

Enhancing Mobile Cloud Computing Security Using Steganography

Hassan Reza, Madhuri Sonawane

School of Aerospace Sciences, Department of Computer Science, University of North Dakota, Grand Forks, ND, USA
Email: reza@aero.und.edu

Received 19 February 2016; accepted 16 July 2016; published 19 July 2016

Abstract

Cloud computing is an emerging and popular method of accessing shared and dynamically configurable resources via the computer network on demand. Cloud computing is excessively used by mobile applications to offload data over the network to the cloud. There are some security and privacy concerns using both mobile devices to offload data to the facilities provided by the cloud providers. One of the critical threats facing cloud users is the unauthorized access by the insiders (cloud administrators) or the justification of location where the cloud providers operating. Although, there exist variety of security mechanisms to prevent unauthorized access by unauthorized user by the cloud administration, but there is no security provision to prevent unauthorized access by the cloud administrators to the client data on the cloud computing. In this paper, we demonstrate how steganography, which is a secrecy method to hide information, can be used to enhance the security and privacy of data (images) maintained on the cloud by mobile applications. Our proposed model works with a key, which is embedded in the image along with the data, to provide an additional layer of security, namely, confidentiality of data. The practicality of the proposed method is represented via a simple case study.

Keywords

Cloud Computing, Mobile Computing, Software Security, Software Privacy, Data Hiding, Steganography, Encryption

1. Introduction

Cloud computing refers to popular method of accessing services and resources via network connections on demand [1]. The popularity of cloud computing, for most part, can be attributed to fee for service and flexibility of

providing services and resources to the customer whenever they these services are needed. The cloud paradigm has significantly eased up front infrastructural and operating cost. However, there are many issues and concerns remained to be addressed when migrating to cloud computing. Examples of these issues include security, scalability, privacy, portability, etc.

The growth of the number of the mobile devices in the past few years has shown that there is a high demand for mobile applications [1]. Mobile devices are considered to be low-end computing. As such, they have limited storage and computing capability compared to the traditional computing platforms such as desktops. Cloud computing has been used as a durable alternative to compensate the inherent limitations of mobile devices by mobile industry [2]. The current approach to increase security and privacy of data work encryption algorithms, negatively affects the performance [3].

Mobile cloud computing (MCC) acting as clients, is benefitting from the cloud computing platform acting as server [4] [5]. Mobile devices and apps became very popular over the past two decades [6]. This is very evident by the exponential growth in the development of mobile devices and systems such as, android, smart phones, PDA's with a variety of mobile computing, networking and security technologies. Mobile computing has three major components [3]: hardware, software and communication.

In mobile cloud computing, the user data are stored on device or cloud. As the internet enabled mobile usage to continue growing, web-based malicious security threat is a serious issue. In this paper, we discuss the working concepts of mobile cloud computing and its various security issues.

In this work, we attempt to address security of mobile cloud computing using mobile devices, because it is very important for customers and providers to retrieve, transmit and retain the data on cloud without breaking any type of secrecy [7]. As discussed in [5] [7], existing security standards and policies [4] are meant to assure the data and access security, but no standards/requirements currently exit to prevent unauthorized access of customer data by the cloud providers. Toward this goal, we have applied techniques from steganography to secure data maintained by the cloud provide. Steganography has been used to hide messages [8] inside some kinds of contents like image, audio or video in such a way that it does not allow anyone to detect that there is a secret message present. Due to today's advanced modern technology, stenography is used on image, text, audio and video [9]. Efficiency of the application is based on the medium used and the maximum data capacity to hide information inside medium.

2. Background: Cloud and Mobile Computing

Cloud computing is one of the popular methods for the users to host and deliver services over the Internet by dynamically providing computing resources [1]. Cloud computing eliminates the overhead of planning ahead for acquiring different resources. The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1]. According to NIST, the key characteristics of cloud computing are:

- On-demand self-service: The users have access and the power to change cloud services online. User can add, delete, or change storage networks and software as needed.
- Broad network access: User can access cloud services using their Smartphone, tablets, laptops, or desktop computers. These devices can be used, wherever they are connected with online access point.
- Resource pooling: The cloud computing enables users to enter and use data within the software, hosted in the cloud at any time, and from any location.
- Elasticity: The cloud computing is flexible and scalable according to the user's needs. User can easily add or remove other users, resources or software features.
- Measured service: Cloud provider can measure storage levels, processing, the number of user accounts and the user are billed accordingly.
- Pricing: Cloud computing cost is based on amount of resources used by the user. Cloud computing is transparent to capture for accurate billing information.
- Quality of service: Cloud computing guarantees, best performance, adequate resources and on round-the-clock availability service for the users.

Cloud Computing services can be classified into three layered service models. These models are: 1) Infrastructure as a service (IaaS), 2) Platform-as-a-Service (PaaS), 3) Software-as-Service (SaaS) [2]. The IaaS model

is based on the provisioning of processing, storage, networks and other fundamental computing resources which are more hardware oriented [10] [11]. This service is mainly used by the system managers. The consumer is able to deploy and run arbitrary software. With infrastructure as a service, the user itself is able to run and manage own operating systems and applications by using virtualization technologies user can also make use of storage systems and/or network devices. The infrastructure management of is done by the service provider of the cloud but still the user has full control of operating systems, applications, storage and partial control over network devices. The advantage IaaS is that there is no need to purchase a server and manage physical data storage, networking manually. Examples: Amazon EC2 for computation power and Amazon S3 for storage provisioning.

The PaaS model allows users to run applications on the infrastructure offered by the service providers. The PaaS requires that the applications are created with programming languages or tools that are supported by the service provider. The management of the infrastructure and operating systems is in the hands of the service provider. While on other hand user has full administrative control over the applications he wants to host on the cloud system [12]. This service provides pre- built application components known as Application Programmable Interface (API). It is commonly used by developers to build the higher level applications. Examples of this model include: Google Application Engine, Force.com.

The SaaS model allow applications and software service are being used on demand The management of the infrastructure, operating systems and the configuration of the application is completely achieved by the service provider. This service is commonly used by the business users. It provides the complete customizable within the limits applications. It is mainly used for achieving specific business task with mainly focusing on end-user requirements. Examples: Google Docs, Microsoft Office Web Applications.

Cloud deployment models refer to how cloud infrastructure are operated and utilized by users, and organizations. According to NIST, cloud deployment models are public cloud (services available to public), private cloud (services are exclusively available to the member of a single organization), community cloud (services are exclusively available to the member of multiple organizations), and hybrid cloud (share feathers of both public and private clouds).

Mobile cloud computing (MCC) refers to the computing paradigm that combines the capability of low end computing devices such as smart phones with the capabilities provided by the cloud computing using network connectivity. The key characteristics of mobile cloud computing are Reliability, Scalability, Security, Agility, device independence, reduced cost of mobiles and mobile services and reduced maintenance [12]. Moreover, mobile cloud computing provides auto-upgrade services to the users devices based on the service demand by the user.

Figure 1 represents the architecture of MCC. In this mode, mobile devices takes the advantages of the services provided by cloud computing. In **Figure 1**, the main components of the MCC architecture are mobile user, mobile device, network connectivity, and cloud service provider [14]. User is responsible for accessing mobile, installing mobile applications, upgrading the applications and operating systems, creating the backup files, downloading and/or uploading information from or to cloud. Cloud service provider mainly provides various services, such as applications and storage, etc. User's data (e.g., images) can be offloaded to the cloud via the mobile network.

Cloud Computing Security Breaches and Issues

The objective of the mobile cloud computing is to make process convenient for mobile user to access and re-

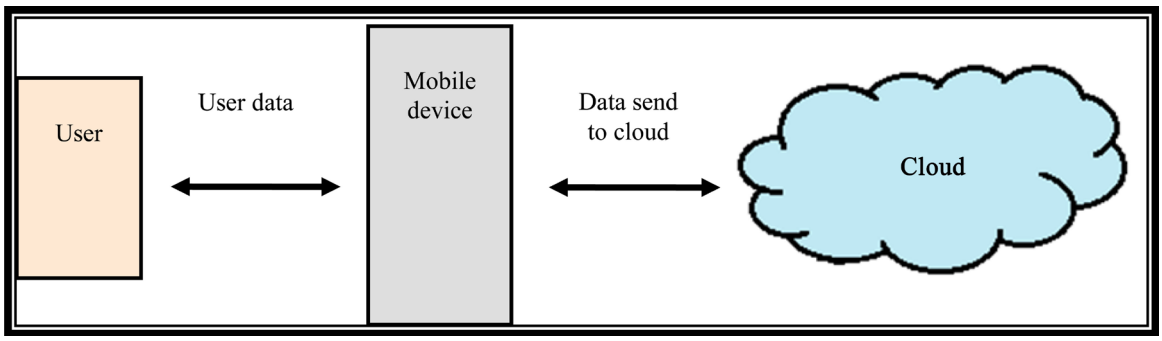

Figure 1. Mobile cloud computing model.

ceive data from the cloud [12]. In spite of many advantages provided by the mobile cloud computing, there are some security challenges exist in the area of mobile and cloud computing. According to [15], major security issues include: 1) Data ownership, which means the legal rights and complete control over data elements, 2) Data privacy, which is the right of an organization (or individual) to determine what data can be shared by who, 3) Data security, which refers to protecting data from malicious use.

Other important issue is the notion of security of data stored in the data storage provided by cloud computing provider. To secure data on the cloud, cloud providers are required to follow security standards and measures [12]. These data security standards are supposed to implement operational security policies and procedures Examples of these policies include: access control, encryption, content assurance, data authentication procedures, and account and user management [16].

In general, when data is stored and offloaded to the cloud, mobile devices may be exposed to the following security threads: 1) In case the mobile device gets stolen or lost, the transmission of un-encrypted data between cloud computing and mobile devices [6] [12] [17]-[20], which may be subject to man-in-the-middle attacked, or data security breach by insider (*i.e.*, cloud administrator).

In case when the mobile devices are stolen (or lost), data from the devices, can be avoided by wiping of mobile device from remote location. To handle man-in-the-middle attack, majority of mobile manufacturers provide feature or security application [2] [5]. In regard to the insider attack by cloud administrator, there are not any viable protection exist. In this work, we are trying to provide additional layer of protection against insider attack. To this end, we are utilizing steganography to enhance the data security offload to the cloud computing.

3. Related Work

There are many different approached of storing data securely over the cloud, using mobile computing such as end-to-end encrypted data transmission, dynamic credential generation, steganography etc.

The stored application or information on cloud raises security issues which are discussed in Bilogrevic [21]. To increase the storage capacity of mobile device, mobile users use cloud storage services. The mobile users do not have any control on the information store on the cloud which causes security and privacy issues [22]-[24].

C. Saravankumar and C. Arun [5] explain cloud computing issues and proposed new cloud computing security model. An important issue of the mobile cloud computing is to secure the user data is addressed in this paper. There are many security standards and policies are available to secure the data such as data privacy, authenticated access to data, third party data protection, but these standards are exist only at the cloud end. It is a critical for the customer as well as provider to store, retrieve and transmit the data over the cloud network in a secure manner. To provide secure system, the authors have proposed the algorithm [5] to develop a customer owned security model. This algorithm is able to send the encrypted data to the provider. The provider can also apply the security by encryption over the customer's data by using the algorithm. The customer's data is secure at both the end. The proposed algorithm uses ASCII and BCD security with steganography that stores the encrypted data in an image file which will be send to the provider end. The security algorithm is using CDM (Common Deployment Model) which also provides an interoperable security services over the cloud. The main objective of the proposed algorithm is to control and send the data in an encrypted manner by the customer to the provider. The provider also maintains the data with a security algorithm to protect the data from unauthorized access.

Z. Al-Khanjari and A. Alani proposed a steganography scheme architectural model to protect data in cloud. Cloud computing systems needs to satisfy interoperability, security, safety, dependability, performance and many other parameters [25]. Security is one of the important issues, discussed and resolved in this paper using protected access control technique which can prevent security problems. Authors are proposing steganography to secure the data in cloud computing. The paper explains that how to hide the data through security pipeline channel. This provides protected access to the data. Steganography will provide safety, dependability, performance, integrity and confidentiality to the data for exchanging data over the network. It is hiding the data when data is requested and displayed. This steganography scheme uses text properties to hide the data, text properties includes font, font metrics, font styles, color and their RGB values, and the x, y location to display data. This steganography architecture supports cloud computing to provide security from unauthorized access. The architecture contains 3 layers physical Layer, data Layer, security Layer [25]. Security layer hides the data through security pipeline channel.

S. Brohi, M. Bamiah, S. Chuprat and J. Manan provide a solution for data privacy issue [26]. In some organization such as healthcare and payment card industry, have a user's personal data which is very important factor,

these organizations can store data on cloud but malicious attackers may steal, view or manipulate client's data. To provide privacy to cloud data storage, authors propose an improved technique which consists of five contributions [26]: resilient role-based access control mechanism; partial homomorphic cryptography; efficient third-party auditing service; data backup and recovery process.

This technique maintains client's data intact and protects them from malicious attackers.

Resilient Role-based Access Control Mechanism - The process starts from this phase and it is responsible for generation of private and public keys by requesting the cloud server for data communication over the internet.

Using Partial Homomorphic Cryptography, data inside the file will be homomorphic-ally encrypted during the uploading process and stored on the cloud in the encrypted format [26]. Whenever this file is required, server needs client's private key to decrypt the selected file. This technique not allows the client to process the data on cloud while it is in the encrypted format [26]. To change the encrypted data, client needs to decrypt the data prior to processing. Here author has used the security features of asymmetric algorithms, he has implemented the homomorphic version of RSA algorithm to encrypt, decrypt and process the encrypted data on cloud.

4. Steganography: Background

Now a day's sender can send the secret data openly using encrypted mail or files to receiver with no fear of reprisals. However there are often cases when this is not allowed when sender or receiver is working for a company that does not allow encrypted email or the local government does not allow encrypted communication. This is where steganography can play a key role. In the simplest form, steganography refers to the method of writing hidden messages in a manner that no one other person but sender and receiver would be able to securely understand and communicate the information hidden in the means of communications (e.g., images) [6] [13] [27]-[29]. The steganography is a channel of communication through which secret data can be transmitted in total secrecy to avoid misuse of data. To this end, steganography covers secret data into some kind of medium like images, audio or video and transmits them in total secrecy from sender to receiver to avoid suspicious attacks. In this paper, we propose a text steganography method for hiding secret textual data and uploading it over cloud.

Figure 2 shows the architecture of steganography. The model consists of the following components: users,

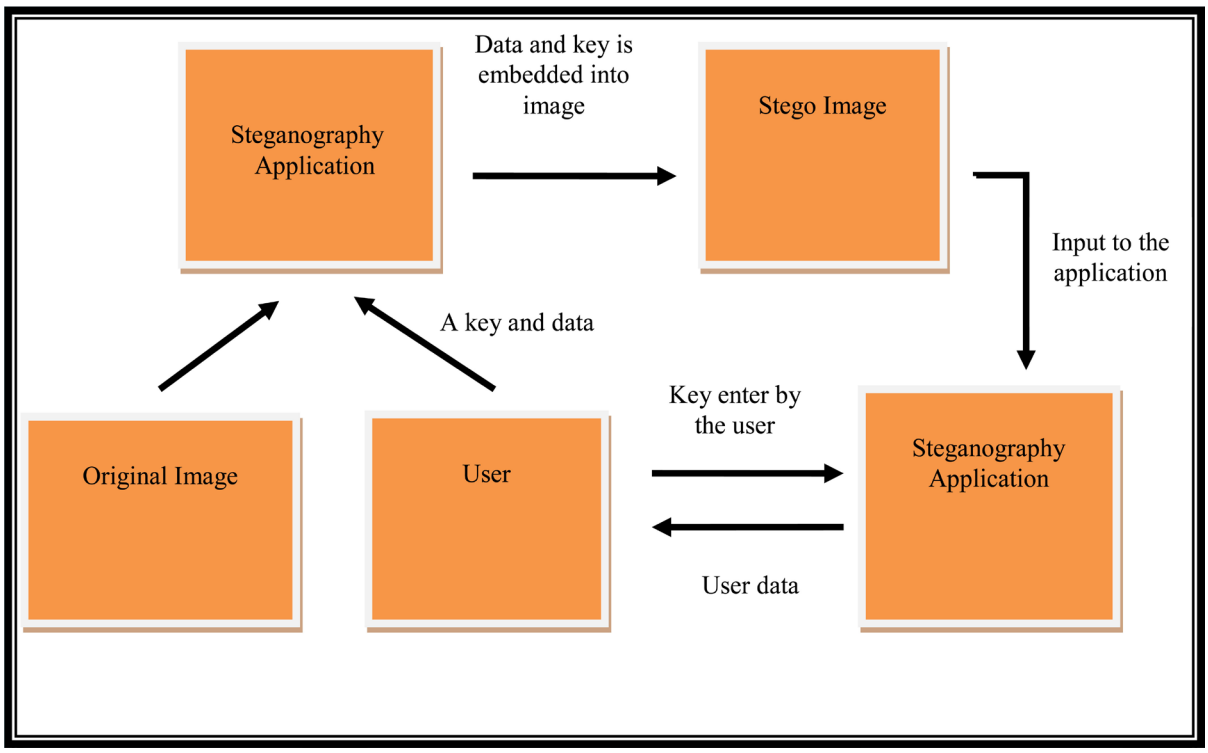

Figure 2. The architecture of Steganography.

who interact with system by inputting data and the key, original image that the sender will use to embed the data, stego-image, which is the image contains embedded key and data, and finally, steganography application, which receives as an input stego-image and user key.

In the steganography model, the user is responsible for selecting any 24-bit image and entering data and the key. In steganography, the classified information aretypically stored in the least significant bits of a digitized file, that means those bits that can be changed in subtle way and hence cannot be detected by the human eye.

After accepting input from the user, the steganography application embeds the key and data into the image selected by the user; this image is called a stego-image. To retrieve data from the image, the stego-image acts as an input to the steganography application. The steganography application retrieves the key from the stego-image and compares it with the user entered image; if both keys are matched then the application displays the embedded data to the user.

Steganography can be classified as: 1) pure steganography, 2) symmetric steganography and 3) asymmetric steganography [30]. Pure steganography does not require any exchange of information. Symmetric steganography does not require exchange of keys prior to sending the messages. Asymmetric steganography does not require to exchange keys prior to sending the messages.

Steganography, for the most part, is dependent on the type of medium being used to hide the information. Medium being commonly used include text, images, audio or video used in network transmissions. Image steganography is generally more preferred media because of its easiness, harmlessness and attraction. Technology advancement in cameras and digital images being saved in cameras and then transfer to PCs [15] has also enhanced many folds. Another thing is the text message hidden in the images does not distort the image. There are some techniques available which change only one bit of an image whose effects is almost negligible on its quality and image looks like unchanged. There are some methods are used to hide information in the media/medium selected for steganography. Some methods are as follows [28]: 1) embedding secret message in text/documents, 2) embedding secret message in audio/video, 3) embedding secret message in images.

To farther enhance secure communication, it is common practice to encrypt the hidden message before placing it in the cover message. However, the hidden message does not need to be encrypted to qualify as steganography. The hidden message can be in plain English. If steganographer decides to have the extra layer of protection then the encryption should provide that extra level of protection. In case, the hidden message is found by unauthorized person (thief), then encryption provides additional level of data protection.

In what follows, we explain the method of embedding secret message in images using pure Steganography approach.

5. The Method Using Steganography

For the mobile users, data security and privacy are key concerns. Cryptography and steganography are basic but popular methods to protect data. Using cryptography, the data is transformed using well-defined algorithm that hopefully makes it hard to read encrypted data without having proper keys.

On the other hand, steganography operates by hiding the message in some kind of medium to transfer to another user in such a way that no one will be able to see or guess the exchange of messages. Some steganography methods are hybrid method combining cryptography and steganography. Combination of cryptography and steganography method may enhance the security of the communication, may affect the performance because these technique demand additional processing that may affect energy consumption. To ease the power consumption, our proposed application applies steganography with an embedded key.

In what follows, we outline the overall process to apply steganography. The process consists of the following steps:

1) Encryption (Optional): The media file which is supposed to be processed will be encrypted in some binary codes. These binary codes depend on the nature of media file. This encryption is different for different files.
2) Data chunking: The encrypted media file is chunked in various parts and this file is to be proceeding for further steganography.
3) Applying steganography: The steganography is done on the chunked encrypted files. Sending chunked files - The chunked files to be sent to receiver and these files will be in the hidden form. This all files are received by the receiver and then are proceed to get the original data.
4) File recombination: The chunked files are recombined to get the whole file so that the receiver can get the

original file.

5) Decryption (optional): The previously recombined file is decrypted to get the original file which is sent from the sender.

Images are the most popular medium to use as a cover for steganography. In the simplest form, an image is a collection of pixels that contains different light intensities [31]. These pixels are referred by numeric forms of a grid and displayed horizontally. Most images are in rectangular shape of pixels and represented as bits and color of the pixel. Each pixel has 8-bits to describe the color [31]. There are different image formats exist and for these different image formats, different steganography algorithms exist. There are mainly three types of image files are used for steganography, 16-bit, 24-bit and 32-bit. Digital color images are usually 24-bit files and uses RGB color model it is also known as true color. RGB color model of the 24-bit image are derived from three primary colors: red, green and blue and each color is represented by 8-bits.

Information can be hidden in many different ways in images. Message insertion in images means simply embed every bit of information in the image. More complex encoding can be done by embedding the message only in "noisy" areas/pixels of image that will attract less attention. The message may also scattered on pixels randomly throughout the cover image.

In general, the most common approaches for information hiding are [8] are: 1) Least Significant Bit (LSB) insertion, 2) Masking and filtering techniques, 3) Algorithms and Transformation.

The least significant bit [15] (LSB) insertion is considered as a common, simple, and efficient algorithm for embedding information in an image [31]. The least significant bit is also called as 8th bit of the bytes inside an image which is changed to a bit of the information which is to hide.

Using a 24-bit image, a bit of each of color (red, green and blue) corresponding to each pixel of image can be used to embed the data, which means each pixel store 3 bytes with 8-bits in each. The message is embedded into the first 8 bytes of the grid and in each byte only the 3-bits are changed to embed the information. So only half of the bits in an image is needed to be modified in order to hide a secret data [9] [29]. Since there are 256 different possible intensities of each color, changing the least significant bit of a pixel should result in small changes in the intensity of the colors. These changes, in turn, cannot be identified by human eye and allows the message to be successfully hidden, stored, and finally transmitted over Internet. When modifying the LSB bits in 8-bit image pointer to enter in the palette are changed. It is really important to remember that a change of even one bit could mean the difference in a shade of red and shade of blue. Change of shades sometimes would be noticeable on displayed image. While in other-hand grey-scale palettes shades is not as pronounced

The main benefit of LSB insertion approach is that the data can be inserted in the pixels but still the human eye would be unable to notice it. While using LSB approach on 8-bit images, more care needs to be taken, as 8-bit format changes can be detected by human eyes as 24-bit format are not. Also, additional care needs to be taken in the selection of the cover image in a way that changes to the data will not be visible in the stego-image. Commonly known images, painting such as the Mona Lisa should be avoided. In most cases, a simple picture of (e.g., dog) would be ideal.

Masking and filtering techniques hide the information by marking the image in a manner similar to paper watermarks. This technique can be applied on 24-bit gray-scale or colored images. Watermarking techniques are more integrated into the image; they may be applied without fear of image destruction. The human visual system cannot detect changes in JPEG images.

The algorithms and transformations technique, on the other hand, use mathematical functions to hide the least bit coefficients in the compression algorithms which reduce the size of images.

Proposed Approach to Secure Data from Cloud Provide

The proposed solution allows a customer to protect its own data by maintained by cloud provider. Although, mobile devices are increasingly essential part of human life, but they are considered as low-end computing with limited processing capability, energy supply, data protection, and storage capacity. As noted previously, it is imperative to consider these inherent limitations of mobile devices when one is attempting to provide additional layer of data protection.

Figure 3 shows the software architecture of the proposed system with the steganography application (SA). The key elements of our model include the following components: User, who select an image and enters key and data, 2) Mobile device (smartphone), which works as an intermediate device bridging the gap between the

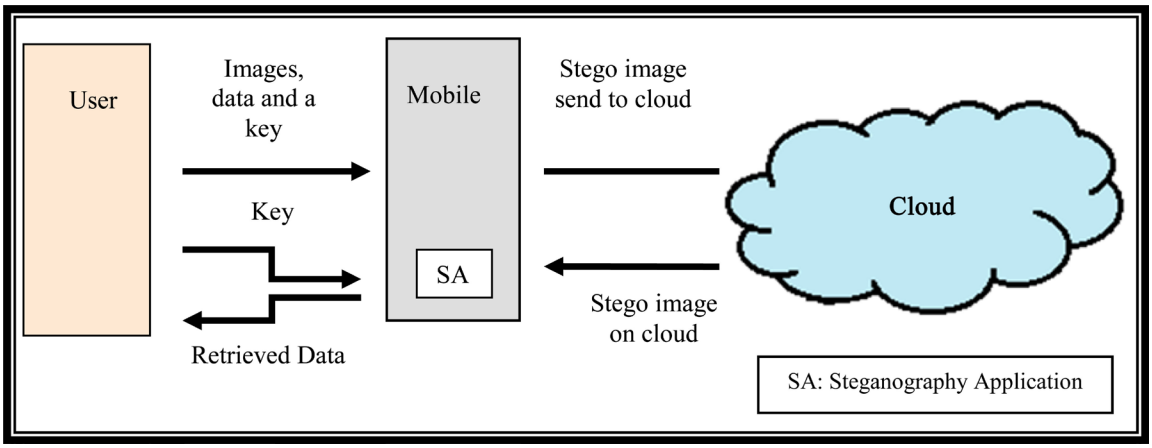

Figure 3. Proposed system.

sender and receiver's information on which the steganography application is running, 3) Steganography application (SA), which is a mobile-application (app) running on the mobile device to embed data and the key in the image given by the user; it then generates a stego-image and retrieves data from the image if user entered key matches, 4) Cloud computing provider providing various service (e.g., SaaS).

The proposed architectural model is based on Client-server architecture [32]; the system is combines the essential features of cloud computing and steganography. As noted previously, in this model, this is the user who is responsible for selecting an image, entering the data and the keys as the input; the input are used by the steganography application, which is configured on the user's mobile device. The steganography application processes all these inputs and creates as an output the stego-image to be stored on the cloud. It is assumed that the mobile device has a connection via internet to access the data maintained on cloud. At the time of data retrieval, the image is fetched from the cloud and again processed by the steganography application to display data to the user if the user entered key matched with the embedded key.

There exists a large body of work aiming at hiding sensitive information in images. Our proposed approach uses 24-bit image steganography to embed data and a key into an image. Different methods of hiding messages work with different types of images. For example, one technique lacks in payload capacity whereas the other approach lacks in robustness.

In this research we have used the least significant bit technique to hide information, which makes the mobile cloud computing application robust and less prone for image distortion. We used 24-bit images because 24-bit images can display more than 16,000 k different combinations that can easily hide data in a way that it will be hard to detect any difference between the modified image and the original image.

To add additional layer of protection, encryption algorithms are used but if the user wants to embed large amounts of information, these algorithms may increase the load on the processor as well as the response time. To overcome this problem, we have used the concept of a key to provide more secure data storage. Using a key, the key first is embedded into an image together with the payload (data). The system will use a specific algorithm to calculate those bytes' location where the key has been stored. Because this app is deployed and used on the user's side, therefore only the user of the system needs to remember this key. As such, we do not need to be concerned about key exchange between the sender and receiver.

The digital image is represented by an array of pixels. These pixels represent the intensities of the three colors: red, green and blue (also known as RGB). In RGB model, a value of each color describes a pixel. In our case, we are using Least Significant Bit (LSB) approach for hiding information into the image.

In what follows, we show how the data embedding process of using LSB is performed. Assuming that the user wants to embed letter "A" into a 24-bit image and the binary value of "A" is 10000011. In 24-bit image each pixel has eight bits for each color in RGB model that is red, green and blue. The user needs to change the least significant bits that require only 3 pixels for hiding 8 bits letter "A". The original three pixels are represented in **Table 1**. Each row of the table represents each pixel and each column represents RGB value of each pixel.

After embedding the binary value of "A" that is 10000011 into the three pixels, starting from the top left byte in the table and going to the right end. Following the same sequence for each row would generate result represented

Table 1. Represents 24-bit word.

	Red	Green	Blue
Pixel 0	00100111	11101001	11001000
Pixel 1	00100111	11001000	11101001
Pixel 2	11001000	00100111	11101001

Table 2. Represents 24-bit word after inserting the letter A.

	Red	Green	Blue
Pixel 0	00100111	11101000	11001000
Pixel 1	00100110	11001000	11101000
Pixel 2	11001001	00100111	11101001

in **Table 2**. For red byte of the pixel 0, last bit is replaced with first bit of letter A and process is continued till the last bit of the letter 'A'. In this example, we have used an 8-bits letter 'A' to replace 9 bytes; the blue byte of pixel 2 remains unchanged. The underline values are the ones which are modified by the LSB transformation method.

The most important features of this application are, the user can use different keys for different information, so even if the thief guesses the key for one stego-image he won't be able to use same key for other images, which reduces the chances of data theft, and if the user loses the mobile device, then the user can access cloud data from any other mobile by simply downloading the "Mobile Cloud Computing" application on that mobile device.

6. Case Study

In recent year's mobile with digitalized applications are widely used and popular due to flexibility and feasibility of the wireless internet. Most of the daily work can be performed easily with the help of mobile internet such as modern ways of communication like Messenger, Whats App, Facebook and Email, handling banking accounts using mobile e-banking.

Now a day's who owns a mobile, text or call more often than directly going to someone's house to convey the message even if house is really close. Email's has replaced for mails. Paper signed up or registration has replaced by online forms etc.

For any kind of online work, we mostly have to sign up and open new account with personal detail so that you can access your account later with username and password. Due to the popularity and comfort of mobile wireless internet access, user prefers opening and accessing new accounts using mobile phones. In this case it is highly possible that user have many accounts and there is high chance of forgetting credentials of those accounts. Hence to be on the safe side, users write down some important information or pass phrase somewhere. This written information may be read or access by another user or it is also possible that user kept this information at house and wanted to access that from remote location which is not possible. To handle this issue, we have proposed solution in which user can store limited amount of information on cloud, by mobile using steganography, which will protect user data from cloud administrator. If user is storing their information on cloud then they can access data from any location without any strain of losing important data on mobile device or any unauthenticated data access.

This application works for small amounts of data per image with low processing power and less battery usage, which eventually increases the performance of the overall application and the mobile device. This approach combines and enhances the trust in mobile computing as well as the efficiency of cloud computing.

Figure 4 shows the Mobile Cloud Computing Application's main page, where a user can select an input and output image path, and enter data and a key to embed into an image. **Figure 5** explains how a user can enter information and an encryption key to embed in the selected image.

Figure 6 shows that using mobile cloud computing application; a user is able to browse for the file location of the original image as well as the file location of the stego-image (message embedded image) using the provided "Browse" button. **Figure 7** and **Figure 8** display a message shown by the application after pressing the "Embed"

button. This message box represents that the process of message encoding and key into the specified image is completed successfully."Browse" button to select the stego-image and enter the key. After pressing the "Retrieve" button, information is retrieved if the entered encryption key matches with the retrieve key from the stego-image.

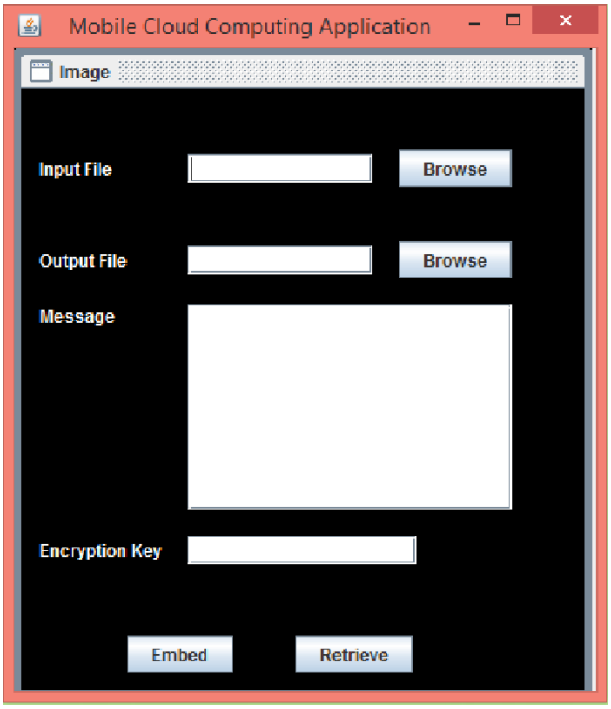

Figure 4. Main page.

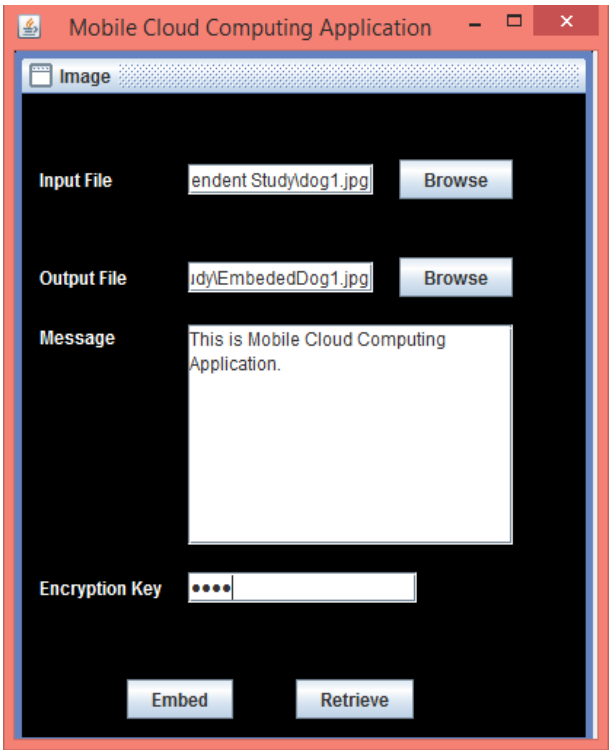

Figure 5. Data acceptance page.

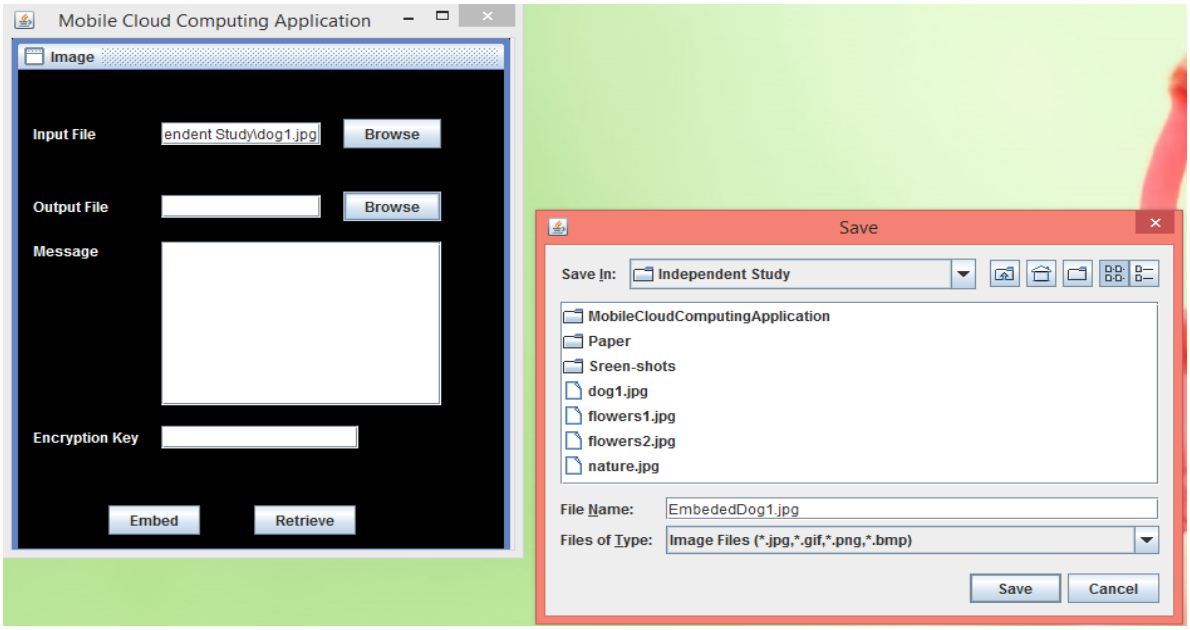

Figure 6. File selection page.

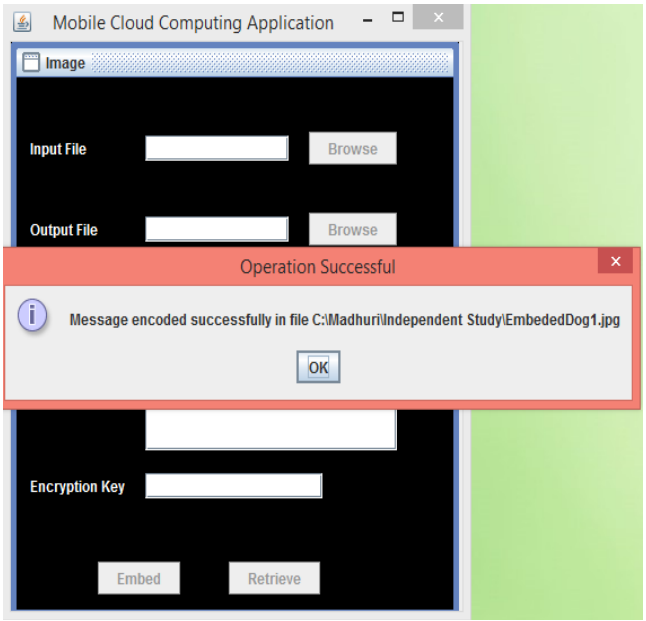

Figure 7. Operation successful message box.

Figure 9 and Figure 11 are the original images and Figure 10 and Figure 12 are the stego-images created after embedding secret message and the key. This figures shows that the images look same before and after embedding the message and key into the image. Image is little distorted but it cannot be recognized by human eyes.

7. Conclusion and Future Work

Mobile cloud computing is one of the mobile technology trends which combine the advantages of both mobile computing and cloud computing, and provides optimal services for mobile devices. Cloud computing is a transformative technology that can change the nature of computing so often, specifically for business purposes. It offers on-demand network access for configurable computing resources like networks, servers, storage, applica-

tions, and different cloud services that can be rapidly installed and uninstalled with minimal management effort.

Many applications are supported by mobile cloud computing such as mobile commerce and mobile healthcare, which contain user sensitive data. Security to this sensitive data is a more important factor in the mobile cloud computing. Due to memory storage issues, this data are usually stored on the cloud. Cloud data are secured against invalid data access and data theft, but technologies are still lacking behind due to the cloud administrator's

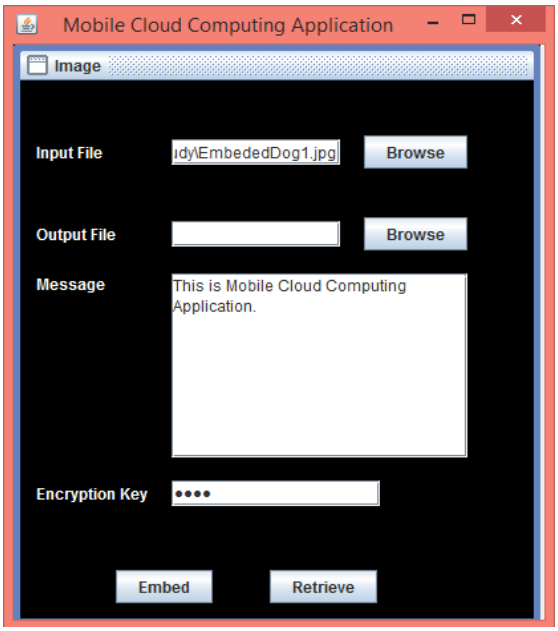

Figure 8. Data retrieval page.

Figure 9. Before using SA.

Figure 10. After using SA.

Figure 11. Before using SA.

Figure 12. After using SA.

invalid data access. Hence, to resolve this issue, we have proposed a "Mobile Cloud Computing" application, which provides secured data storage through mobile on the cloud against the cloud administrator by using steganography application which improves performance of mobile cloud computing. This steganography application can be used on networks for data security without using third party interference. The mobile cloud computing application is able to embed only limited amounts of data into images. In the future, we can extend this capability from a few words to huge data files by replacing the steganography medium that is, images with audio or video files. The proposed system will work perfectly as long as a user remembers the key, but if he loses the key, then the system does not have any provision for recovering or guessing the key, so in this case a user might lose the data. This issue will have to be addressed in the future. The proposed system is efficient and legal for the client as long as the cloud administrator doesn't have restrictions about a client's data. As this system is hiding the original data, a user may abuse this feature and can store illegal or unethical data. As of now, the proposed system does not have any remedy for this issue. In the future, cloud management systems and proposed models may work in parallel for smooth and legal data storage function.

References

[1] Gupta, P. and Gupta, S. (2012) Mobile Cloud Computing: The Future of Cloud. *International Journal of Advanced Research in Electrical Electronics and Instrumentation Engineering*, **1**, 134-145.

[2] Bheda, H. and Lakhani, J. (2013) Application Processing Approach for Smart Mobile Devices in Mobile Cloud Computing. *International Journal of Software Engineering and Knowledge Engineering*, **3**, 1046-1055.

[3] Buyya, R., Yeo, C. and Venugopal, S. (2008) Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering it Services as Computing Utilities in High Performance Computing and Communications. *The*10*th IEEE International Conference on IEEE*, 5-13.

[4] Donald, C. and Arockiam, O.L. (2013) Mobile Cloud Security Issues and Challenges: A Perspective. St. Joseph's College Tiruchirappalli, Department of Computer Science, Tamil Nadu.

[5] Saravankumar, C. and Arun, C. (2014) An Efficient ASCII-BCD Based Steganography for Cloud Security Using Common Development Model. *Journal of Theoretical and Applied Information Technology*, **65**, 1992-8645.

[6] Prasad, R., Gyani, J. and Murti, P. (2012) Mobile Cloud Computing: Implications and Challenge. *Journal of Information Engineering and Applications*, **2**, 7-15.

[7] Juneja, M. and Singh, P. (2014) Improved LSB Based Steganography Techniques for Color Images in Spatial Domain. *International Journal of Network Security*, **16**, 366-376.

[8] Kumar, A. and Pooja, K. (2010) Steganography: A Data Hiding Technique. *International Journal of Computer Applications*, **9**, 975-8887. http://dx.doi.org/10.5120/1398-1887

[9] Ross, A. and Fabien, P. (1998) On the Limits of Steganography. *IEEE Journal of Selected Areas in Communications*, **16**, 474-481.

[10] Foster, I., Zhao, Y., Raicu, I. and Lu, S. (2008) Cloud Computing and Grid Computing 360-Degree Compared. *Grid Computing Environments Workshop*, **2008**, 1-10. http://dx.doi.org/10.1109/gce.2008.4738445

[11] Buyya, R., Yeo, C., Venugopal, S., Broberg, J. and Brandic, I. (2009) Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing. *The 5th Utility Future Generation Computer Systems*, **25**, 599-616. http://dx.doi.org/10.1016/j.future.2008.12.001

[12] Bahar, A., Habib, M. and Islam, M. (2013) Security Architecture for Mobile Cloud Computing. *International Journal of Scientific Knowledge*, **3**, 11-17.

[13] Nasab, M. and Shafiei, B. (2011) Steganography in Programming. *Australian Journal of Basic and Applied Sciences*, **5**, 1496-1499.

[14] Shamim, S., Sarker, A. and Bahar, A. (2015) A Review on Mobile Cloud Computing. *International Journal of Computer Applications*, **113**, 4-9. http://dx.doi.org/10.5120/19908-1883

[15] Kekre, H.B., Athawale, A. and Halarnkar, P.N. (2008) Increased Capacity of Information Hiding in LSB's Method for Text and Image. *International Journal of Electrical*, *Computer*, *and Systems Engineering*, **2**, 246-249.

[16] Sahu, D., Sharma, S., Dubey, V. and Tripathi, A. (2012) Cloud Computing in Mobile Applications. *International Journal of Scientific and Research Publications*, **2**, 1-9.

[17] Huang, D., Zhou, Z., Xu, L., Xing, T. and Zhong, Y. (2011) Secure Data Processing Framework for Mobile Cloud Computing. *IEEE Conference on Computer Communications Workshops* (*INFOCOM WKSHPS*), Shanghai, 10-15 April 2011, 620-624. http://dx.doi.org/10.1109/infcomw.2011.5928886

[18] Satyanarayanan, M. (1996) Fundamental Challenges in Mobile Computing. 15*th Annual ACM Symposium on Principles of Distributed Computing*, Philadelphia, 23-26 May 1996, 1-7. http://dx.doi.org/10.1145/248052.248053

[19] Oberheide, J., Veeraraghavan, K., Cooke, E., Flinn, J. and Jahanian, F. (2008) Virtualized In-Cloud Security Services for Mobile Devices. 1*st Workshop on Virtualization in Mobile Computing*, Breckenridge, 17-20 June 2008, 31-35. http://dx.doi.org/10.1145/1622103.1629656

[20] Portokalidis, G., Homburg, P., Anagnostakis, K. and Bos, H. (2010) Paranoid Android: Versatile Protection for Smartphones. 26*th Annual Computer Security Application Conference* (*ACSAC*), Los Angeles, 5-9 December 2016, 347-356. http://dx.doi.org/10.1145/1920261.1920313

[21] Bilogrevic, I., Jadliwala, M., Kumar, P., Walia, S., Hubaux, J., Aad, I. and Niemi, V. (2011) Meetings through the Cloud: Privacy-Preserving Scheduling on Mobile Devices. *Journal of Systems and Software*, **11**, 1910-1927. http://dx.doi.org/10.1016/j.jss.2011.04.027

[22] Ren, W., Yu, L., Gao, R. and Xiong, F. (2011) Lightweight and Compromise Resilient Storage Outsourcing with Distributed Secure Accessibility in Mobile Cloud Computing. *Tsinghua Science and Technology*, **16**, 520-528. http://dx.doi.org/10.1016/S1007-0214(11)70070-0

[23] Yang, J., Wang, H., Wang, J., Tan, C. and Yu, D. (2011) Provable Data Possession of Resource Constrained Mobile Devices in Cloud Computing. *Journal of Networks*, **6**, 1033-1040. http://dx.doi.org/10.4304/jnw.6.7.1033-1040

[24] Tysowski, P. and Hasan, M. (2011) Re-Encryption-Based Key Management towards Secure and Scalable Mobile Applications in Clouds. IACR Cryptology Eprint Archival, 668-678.

[25] Al-Khanjari, Z. and Alani, A. (2014) Developing Secured Interoperable Cloud Computing Services. *The European Interdisciplinary Forum* 2014 (*EIF* 2014), Vilnius, 18-19 June 2014, 341-350.

[26] Brohi, S., Bamiah, M., Chuprat, S. and Manan, J. (2014) Design and Implementation of a Privacy Preserved Off-Premises Cloud Storage. *Journal of Computer Science*, **10**, 210-223. http://dx.doi.org/10.3844/jcssp.2014.210.223

[27] Bassil, Y. (2012) A Text Steganography Method Using Pangram and Image Mediums. *International Journal of Scientific & Engineering Research*, **3**, 2229-5518.

[28] Bender, W., Gruhl, D., Morimoto, N. and Lu, A. (1996) Techniques for Data Hiding. *IBM Systems Journal*, **35**, 313-336. http://dx.doi.org/10.1147/sj.353.0313

[29] Wang, H. and Wang, S. (2004) Cyber Warfare: Steganography vs. Steganalysis. *Communications of the ACM*, **47**, 76-82. http://dx.doi.org/10.1145/1022594.1022597

[30] Mahajan, S. and Singh, A. (2012) A Review of Methods and Approach for Secure Steganography. *International Jour-*

nal of Advanced Research in Computer Science and Software Engineering, **2**, 484-488.

[31] Johnson, N. and Jajodia, S. (1998) Exploring Steganography: Seeing the Unseen. *Computer*, **31**, 26-34. http://dx.doi.org/10.1109/MC.1998.4655281

[32] Shaw, M. and Garlan, D. (1996) Software Architecture: Perspective on an Emerging Discipline. Prentice Hall, Upper Saddle River.