International Journal of Cloud Computing and Services Science (IJ-CLOSER)
Vol.3, No.1, February 2014, pp. 67~78
ISSN: 2089-3337

Security: Issues and Framework Consideration Criteria in Mobile Cloud Computing

***Waziri Onomza VictorPhD, **Joshua Abah, ***Olumide Sunday Adewale,PhD, ****Muhammad Bashir AbdullahiPhD, ******Arthur M. Ume, PhD**
* Departement of Cyber Security, Federal University of Technology Minna, Nigeria.
** Departement of Computer Computer Science, Federal University of Technology Minna, Nigeri.
*** Departement of Computer Computer Science, Federal University of Technology Akure, Nigeri.
**** Departement of Information and Media Technology, Federal University of Technology Minna, Nigeri.
***** Departement of Computer Computer Science, Federal University of Technology Minna, Nigeri.

Article Info

Article history:

Received Jun 12th, 2013
Revised Aug 20th, 2013
Accepted Aug 26th, 2013

Keyword:

Privacy
Mobile cloud computing
Malware
Security
Threats

ABSTRACT

Mobile cloud computing is increasingly becoming popular among mobile users as a model for transparent elastic augumentation of mobile devices capabilities through ubiquitous wireless access to cloud storage and computing resources, with context-aware dynamic adjusting of offloading in respect to change in operating conditions while preserving available sensing and interactivity capabilities of mobile devices. The security issues of mobile cloud computing is a complex integration of cloud computing, wireless networks, mobile devices and web technologies. Irrespective of the high level of advertisement and publicity of mobile cloud computing, the degree of take-up and adoption is still low. This low adoption has been attributed to the risks associated with security and privacy. Protecting user privacy and data/application secrecy is key to establishing and maintaining consumer’s trust in mobile cloud computing. Security threats have become a challenging factor to the adoption of mobile cloud computing eventhough efforts are being put in place by researchers and the academia to ensure a secure mobile cloud computing environments and infractrustures. Regardless of these, mobile cloud computing environments and infrastructures have remained vulnerable with existing security issues. This paper introduces mobile cloud computing security issues and security framework consideration criteria. It further review and identifies the potential problems and current proposed work to secure mobile cloud computing.

Corresponding Author:
Dr. Waziri Onomza Waziri
School of ICT,
Federal University of Technology, Minna
Minna-Nigeria.
Email: victor.waziri@futminna.edu

1. INTRODUCTION (10 PT)

Mobile cloud computing is increasingly becoming popular among mobile users as a model for transparent elastic augumentation of mobile devices capabilities through ubiquitous wireless access to cloud storage and computing resources, with context-aware dynamic adjusting of offloading in respect to change in operating conditions while preserving available sensing and interactivity capabilities of mobile devices [1]. The more and more information is placed into the cloud by individual and enterprise, the more security issues grow and rise. Mobile cloud computing integrates technologies such as cloud computing, wireless networks, mobile devices and web technologies [2] as a result, the security issues of mobile cloud is inherited from these constituent technologies.

Irrespective of the high level of advertisement and publicity of mobile cloud computing, the degree of take-up is still low [3]. This low adoption has been attributed to the risks associated with security, privacy and trust. Protecting user privacy and data/application secrecy is key to establishing and maintaining consumer's trust in mobile cloud computing [4], [5]. Security threats have become a challenging factor to the adoption of mobile cloud computing eventhough efforts are being put in place by researchers and the academia to ensure a secure mobile cloud computing environments and infractrustures [3]. Regardless of these, mobile cloud computing environments and infrastructures have remained vulnerable with existing security issues; a never ending issues in mobile cloud computing [1]. This paper discuss the security framework in mobile cloud and the criteria for their evaluation, it further identifies security issues in mobile cloud computing and current work proposed to secure mobile cloud computing.

The rest of the paper is as follow; section 2 portrays the general review of other works based on the mobile cloud security, section 3 deals with related security issues in Mobile cloud computing, section 4

2.0 Related Works

Mobile cloud computing involves the usage of mobile devices that represent compact mobile computer hand-held [6]. This allows us to apply known security definitions and principles to them. Beginning with the term "Security" itself, one interpretation of this word is the condition of being protected against danger or loss [6]. The Department of Defence in [7] defines security as *"A condition that results from the establishment and maintenance of protective measures that ensures a state of inviolability from hostile acts or influences."* Similarly, [9] states that "*security is the process of maintaining an acceptable level of perceived risk where the security process revolves around four steps: assessment, protection, detection, and response.*"

2.1 Security Goals

[8] introduces the term "security goal" to be able to describe objectives that have to be achieved in order to state a computer system or network as secure. These goals are confidentiality, integrity, and availability- the Traid. These goals form the basis for consideration of any security framework. A summary on these terms is given in table 2.1.

Table 2.1: A Summary of Security Goals

Confidentiality	This implies that data that is transmitted or stored should only be revealed to an intended audience
Integrity	Integrity connotes that modifications should be detectable and the creator should be identifiable
Availability	This mean that services should be available and functionally available to the users

2.1.1 Confidentiality

According to [11], confidentiality refers to preserving authorized information, access and disclosure that includes the means for protecting personal privacy and proprietary information of the user's data. Generally speaking, confidentiality refers to limiting access to data and information to authorized persons. In case of computer systems, authentication methods like user name and password or biometric data recognition can only be authorized by authenticated users. The United States' National Institute for Standards and Technology (NIST) states that a loss of confidentiality is the unauthorized disclosure of information [10]. An example of keeping confidentiality on a certain file is to control access to it through user file system rights. A certain user can be assigned sole ownership and right to read, write, and execute the file. An example for losing confidentiality is, if an attacker is able to escalate his system rights to root level. Modern confidentiality is achived through cryptology and steganography using secure keys.

2.1.2 Integrity

Integrity refers to guarding against improper information modification or destruction, and it includes ensuring information non-repudiation and unauthentication [11]. Bishop [8] states that integrity includes data integrity and origin integrity. Data integrity assures that the data is free of modifications or corruptions. Origin integrity guarantees that the source of data and information is marked correctly. He further explains that integrity methods fall into two classes: prevention mechanisms and detection mechanisms. Prevention mechanisms aim at maintaining integrity while detection mechanisms try to identify possible alteration of the data and information. NIST [10], states that a loss of integrity is the unauthorized modification or destruction of information. An example for proving existing data integrity might be realised by checking a created collision-free hash code on a certain file.

2.1.3 Availability

Describes in [11], provides a definition for availability as ensuring timely and reliable access to and use of information. Hence, availability describes whether a resource of information can be used in a timely manner or not. NIST [10] describes that a loss of availability is the disruption of access to or use of information or an information system. Denial-of-Service (DoS) attacks are a common example for disrupting online service and system resources. Besides obvious DoS attacks, availability can also be harmed by unintended action.

3.0 Security Issues in Mobile Cloud Computing

This paper describes cloud computing security therefore; background information of relevant security principles is presented. Since mobile cloud computing is a combination of mobile networks and cloud computing [12], [2] security threats of mobile cloud computing could be divided into three; security threats to mobile devices, security threats to the cloud platform and application containers and security threats to communication channels [4], [2]. Hence, security whether of cloud or of mobile devices is explained through listing prevalent threats and corresponding security measures to them [6].

The protection of user’s privacy and data/information secrecy from adversary is a key to establish and maintaining consumer’s trust in the mobile platform, especially in mobile cloud computing [5]. In the following, the security related issues in mobile cloud computing is introduced in three categories and solutions to address these issues are reviewed.

3.1 Security Issues Relating to Mobile Devices

As far as mobile devices are concerned, security remains a key concern. As if a device gets stolen or misplaced, crucial data may be compromised. Data misuse from stolen/misplaced devices can be avoided by wiping of mobile devices remotely. This feature is generally provided by most of the mobile manufacturers and wireless carriers [13]. Mobile devices such as PDAs, cellular phones, smart phones etc. are vulnerable to numerous security threats like malicious codes (e.g., viruses, worms, and Trojan horses). Global Positioning System (GPS) of mobile devices could also raise privacy issues for subscribers. The following security issues relating mobile devices are identified.

a. **Privacy and Confidentiality**: Providing private information such as indicating your current location and users’ important information creates scenarios for privacy issues. With the advantages of GPS positioning devices, the number of mobile users using location based services (LBS) increases. However, the LBS face a privacy issue when mobile users provide private information such as their current location [5]. This problem becomes even worse if an adversary knows the users’ important information. Location Trusted Servers (LTS) [14] is presented to address this issue. As shown in fig. 2.1, after receiving the mobile user’s request, LTS gathers their location information in a certain area and cloaks the information called ‘cloak region’ based on k-anonymity concept [15], [5] to conceal the user’s information. The ‘cloaked region’ is sent to LBS, so LBS know general information about the users but cannot identify them. [16] Pointed out the problem that if LTS reveals the users’ information, or if LTS colludes with LBS, the user’s information will be in danger. The authors propose to generate the ‘cloaked region’ on mobile devices based on Casper Cloaking Algorithm [17]. Meanwhile, gathering the information of other users around the sender will be done on the cloud to reduce cost and improve speed and scalability. When launching the program on the sender’s mobile devices, the program will require the cloud to provide information about surrounding users. After that, the mobile client will generate the ‘cloaked region’ to the LBS. In this way, both LTS and LBS cannot know the sender’s information [5].

There are various policies and schemes such as Fair Information Practice Principles (FIPP) being proposed which requires rigorous controls and procedures to protect the privacy of individuals [18]. Risk of privacy exposure, identity theft, and fraud can be reduced by implementing enhanced protection measures for sharing data in interconnected systems, implementing monitoring capabilities and protocols, and educating users about proper social media safe surfing [18]. By establishing policies regarding use of social media and implementing processes to protect their infrastructures from unauthorized use of social media an organization can protect themselves from serious legal and security-related problems. Otherwise their information infrastructure and reputation both will be irreparably damaged.

Encryption provides most effective way to maintain integrity and confidentiality of information. Encryption favours data storage and transport but it fundamentally prevents data processing. Therefore, initially it was quite useless to send encrypted data to cloud providers for processing. But this challenge has been met by homomorphic cryptography (HC) which ensures that operations performed on an encrypted text results in an encrypted version of the processed text [19].

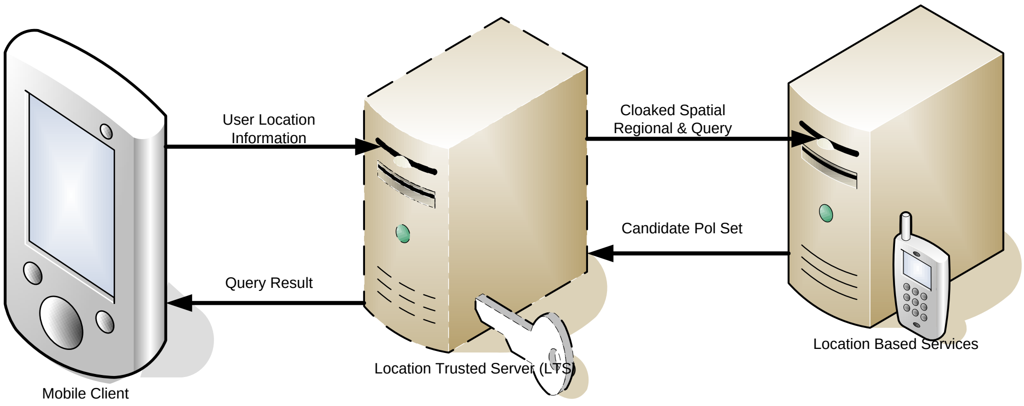
User Location Information
Cloaked Spatial Regional & Query
Candidate Pol Set
Query Result
Location Trusted Server (LTS)
Location Based Services
Mobile Client

Figure 1: Overall Architecture of Spatial Cloaking [5].

b. Security for Mobile Applications

The simplest way to detect security threats of any mobile device is by installing and running security software (like Kaspersky, McAfee, and AVG antivirus programs etc.). However, since mobile devices have limited processing power and energy supply, protecting them from the threats is more difficult than that of resourceful device like the PC [18]. Several approaches have been developed for example; since it is impossible to keep running antivirus programs on mobile device as it reduces the battery lifetime, [20], propose that we can move the threat detection capabilities to clouds. Before mobile users could use a certain application, it should go through some level of threat evaluation. All file activities to be sent to mobile devices will be verified if it malicious or not. This paradigm is an extension of the existing Cloud Anti-virus platform that provides an in-cloud service for malware detection. The advantage of in-cloud detection of malware enables the use of multiple antivirus engines in parallel by hosting them in virtualized containers [21], [5]. However, to apply CloudAV platform for the mobile environment, a mobile agent should be improved and customized to fit in the mobile devices. [20] Builds a mobile agent to interact with the CloudAV network service for the Linux-based Maemo platform implemented on a Nokia N800 mobile device. The mobile agent is deployed in Python and uses the [22] framework to interpose on the system events. [23] Demonstrates the efficiency of using cloud computing for detecting malicious software on mobile devices. They presented a paradigm in which attack detection for smart phone is performed on a remote server in the cloud. Similarly, instead of running an antivirus program locally, the smart phone records only a minimal execution trace and transmits it to the security server in the cloud. This approach therefore enhances the efficiency of detecting malware and also improve battery lifetime up to 30%. Although storing a large amount of data/applications on a cloud has its own benefits but integrity, authentication and digital rights of data/applications should be taken into consideration [5].

3.2 Security Issues Relating to Cloud Platform and Application Containers

Although both mobile users and application developers benefit from storing a large amount of data/applications on a cloud, they should be careful of dealing with the data/applications in terms of their integrity, authentication, and digital rights. The data related issues in mobile cloud computing is as follows:

a. **Integrity:** Mobile users are often concerned about their data integrity on the cloud. Several solutions are proposed to address this issue [24], [25]. However, such solutions do not take into consideration the energy consumption of mobile users. [25] Considers the energy consumption issue. This scheme consists of three main components: a mobile client, a cloud storage service, and a trusted third party. The scheme performs three phases: the initialization, update and verification. In the first phase, files (F_x) that needs to be sent to the cloud will be assigned with a message authentication code ($MACF_x$). These $MACF_x$ will be stored locally, while the files will be sent and stored on the cloud. In the update phase, a case where the user want to insert the data into file ($F_{x)}$ is considered. The cloud then sends the file (F_x) to this user. At the same time, the cloud also sends a requirement to the Trusted Crypto Coprocessor (TCC) to generate $MAC'F_{x.}$ Trusted

Crypto Coprocessor then sends $MAC'F_x$ to the client to verify F_x by comparing it with $MACF_x$. If everything is properly authenticated, the user can insert/delete data. Finally, the mobile client can request the integrity verification of a file, collection of files, or the whole file system stored in the cloud. This phase starts when the user sends a requirement to verify integrity of files to TCC. The TCC then retrieves files that need to be checked from the cloud and generates $MAC'F_x$ to send to the client. The client only compares the retrieved $MAC'F_x$ and $MACF_x$ that are stored on its device to verify the integrity of such files. This technique saves both energy for the mobile device and bandwidth for the communication network [5], [2].

b. **Authentication:** [17] Presents an authentication method using cloud computing to secure the data access suitable for mobile environments. This scheme combines TrustCube [26] and implicit authentication [27], [28] to authenticate the mobile client. TrustCube is a policy-based cloud authentication platform using the open standards, and it supports the integration of various authentication methods [5]. The authors build an implicit authentication system using mobile data (e.g., calling logs, SMS Message, Website access, and location) for existing mobile environment. The system requires input constraints that make it difficult for mobile users to use complex passwords. As a result, this often leads to the use of simple and short passwords or personal identification numbers (PINs). Figure 2 shows the system architecture and how the system secures the user's access. When a web server receives a request from a mobile client, the web server redirects the request to the integrated authenticated (IA) service along with the details of the request. The IA service retrieves the policy for the access request, extracts the information that needs to be collected, and then sends an inquiry to the IA server through the trusted network connect protocol. The IA server receives the inquiry, generates a report and sends it back to the IA service. After that, the IA service applies the authentication rule in the policy and determines the authentication result and sends the authentication result back to the web server. Based on the authentication result, the web server either provides the service or denies the request.

c. **Digital Rights Management**: The unstructured digital contents (e.g., video, image, audio, and e-book) have often been pirated and illegally distributed. Protecting these contents from illegal access is of crucial importance to the content providers in mobile cloud computing like traditional cloud computing and peer-to-peer networks. [29] Proposes Phosphor, a cloud-based mobile digital rights management (DRM) scheme with a subscriber identity module (SIM) card in mobile phone to improve the flexibility and reduce the vulnerability of its security at a low cost. The Authors design a licence state word (LSW) located in a SIM card and the LSW protocol based on the application protocol data unit (APDU) command. In addition, the cloud-based DRM with an efficient unstructured data management service can meet the performance requirement with high elasticity [5]. Thus, when a mobile user receives the encrypted data (e.g., video stream) from the content server via real-time support protocol, the user then uses the decryption key from a SIM card via APDU command to decode. If the decoding is successful, the mobile user can watch this video on his/her phone. The drawback of this solution is that it is still based on the SIM card of the mobile phone; so, it cannot be applied for other kinds of access; that is, a laptop using Wi-Fi to access these contents [5], [2].

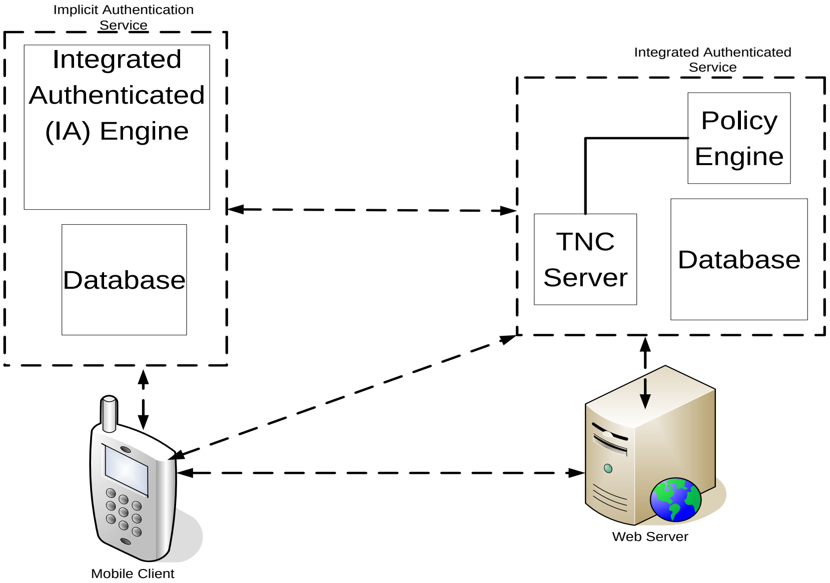
Implicit Authentication Service
Integrated Authenticated (IA) Engine
Database
Integrated Authenticated Service
Policy Engine
TNC Server
Database
Mobile Client
Web Server

Figure3.1: TrustCube Architecture

4.0 Security Issues Relating to Communication Channels

a. **Network Monitoring:** In addition to latency and bandwidth problems network performance monitoring is also an important issue which need proper concern and care [18]. It is critical to have a dynamic cloud performance system that can allow traffic re-routing, access swapping and handover. With all these key challenges given mobile computing is still viable business and is being preferred by more cloud users.

b. **Malicious Attacks:** All networks are susceptible to one or more malicious attacks. As more external website are being accessed, malicious actors will have more opportunities to access the network and operational data of users. Implementing security controls across all Web 2.0 servers and verifying these rigorous security controls can reduce the threats to internal networks and operational data. Additionally, separating Web 2.0 servers from other internal servers may further mitigate the threat of unauthorized access to information through social media tools and Websites [18]. Some of the potential attack vectors criminals may attempt according to [18] include:

i. **Man-in-the-middle Cryptographic Attacks**: This attack is carried out when an attacker places himself between two users. In this kind of attack, attacker places himself in the communication path and after that, it is up to him what to do, he can intercept and modify communication.

ii. **Denial of Service (DoS) Attacks:** The cloud is more susceptible to DoS attacks because more than one client can access cloud at the same time, which makes DoS attack much more damaging. Twitter has suffered a devastating DoS attack in 2009 [18].

iii. Side Channel Attacks: In this kind of attacks a malicious virtual machine is placed in close proximity of a target cloud server to compromise the cloud security and then a side channel attack is launched.

iv. **Authentication Attacks**: Authentication is one of the weak points in case of hosted and virtual services and is generally been targeted. A user can be authenticated in number of ways and these mechanisms and methods which are used to secure the authentication process are frequently been targeted by the attackers.

4.1 Security Threats

The goals of security presented in table 4.1 can be harmed through the following threats [8], [6]: eavesdropping, modification, masquerading and repudiation, denial of receipt, delay, and denial-of-service. A summary on these terms is provided in table 2. A threat is a potential violation of security; meaning that the violation does not actually need to occur but need to be protected against [8]. According to [8], actions that lead to a violation are called attacks; those who perform them are called attackers.

Table4.1: Security Threats

Eavesdropping or Snooping	This occur when an entity reads information that it is not intended to read
Modification or Alteration	This is a situation in which data is being altered or destroyed.
Masquerading or Spoofing	This is when an entity claims to be another (impersonation).
Repudiation	This is a situation in which an entity falsely denies participation in an act.
Denial of receipt	This happens when an entity falsely claim not to have received a delivery of object.
Delay	This is when the delivery of an object is delayed.
Denial of service	This could be defined as any action that aims to reduce the availability and/or correct functioning of services or systems.

a. **Eavesdropping**: Eavesdropping describes the unauthorized interception of information and is also called snooping [6]. Example of eavesdropping are: reading mails that is not addressed to one or monitoring (wireless) network traffic, e.g. for capturing user-name and passwords. In all cases, eavesdropping is passive. Measures to maintain confidentiality can counter this threat [8].

b. **Modification:** Modification describes the unauthorized changes of information and is also known as alteration according to [8]. Since integrity measures address the threat of modification, the same examples apply here: a student that breaks into the computer of his/her teacher in order to alter a list of grades represents the modification threat [6].

c. **Masquerading:** The threat of masquerading also called spoofing is given whenever an entity claims to be another entity [6]. A very simple illustration is the usage of eavesdropped account login credentials. A common real life example is the usage of faked identity cards by under-age persons in order to buy alcohol. Masquerading is addressed by methods that maintain integrity [8].

d. Repudiation: repudiation is the threat that an entity falsely denies participation in an act is called repudiation of origin. An example of this kind of threat which is also given in [8] is if a customer orders an expensive product and denies having ordered it when it gets delivered. Integrity mechanisms cope with this threat.

e. **Denial of Receipt**: if an entity claims that is did not receive information although it did, this is described by [8] as denial of receipt. Using a similar example as before: if a customer receives an expensive product but denies this by asking the vendor whether it was already shipped or not, this can be seen as denial of receipt.

f. **Delay:** Delay is a threat that includes all actions that lead to a delay of delivery of an object [6]. An attacker can e.g. delay the sending of an email that warns employees of a company not to use a certain service since it was misused for phishing purpose right until the people use the service. Availability methods target this threat [8].

g. **Denial of Service:** Denial of service is a threat that bases on preventing objects or services to be used at a certain or any time [6]. Denial of service attacks can be realized through exploiting communication protocol flaws that leads to states not allowing the system to respond (e.g., timeouts). This threat is of special interest whenever companies or institutions are relaying on responsiveness of their services, e.g., in case of online shops or online trading. The common type of DoS attack occurs when an attacker floods a network with excessive requests to the target server until the server is unable to provide services to nornal user [30], [31]. There are many methods to perform a DoS attack such as SYN flood. The SYN flood exploits the TCP 3-way handshake by initialising request connections to the target server and ignoring the acknowledgement (ACK) from the server. This makes the server to wait for ACK from the attacker, wasting time and resources until eventually the server does not have enough resources to provide services to normal clients [30].

While analyzing security it is important to focus on the attack model. *Attack model* is analysis of capabilities of an attacker and what are attacker’s limits [35]. The attacker can be a passive attacker who does not alter the content or an active attacker who might alter or remove the content. The general goals of the attacker are [35]:

i. *Eavesdropping*: The attacker gains access to the conversation between the user using the mobile phone and the base station. When an attacker is eavesdropping on a communication, it is referred as sniffing or snooping.

ii. *Availability attacks*: The attack which prevents the use of mobile phone by jamming the communication by device and the base station is referred to as Availability attack.

iii. *Privacy attacks*: Attacks that focus on getting the information like about location, usage pattern etc. about a user is an attack on his/her privacy.

iv. *Impersonation attacks*: It is the ability of an attacker to use the service of Mobile Network Operator (MNO) without being billed for the usage.

[36], [35] classified mobile threat model into three categories; malware, personal spyware and grayware.

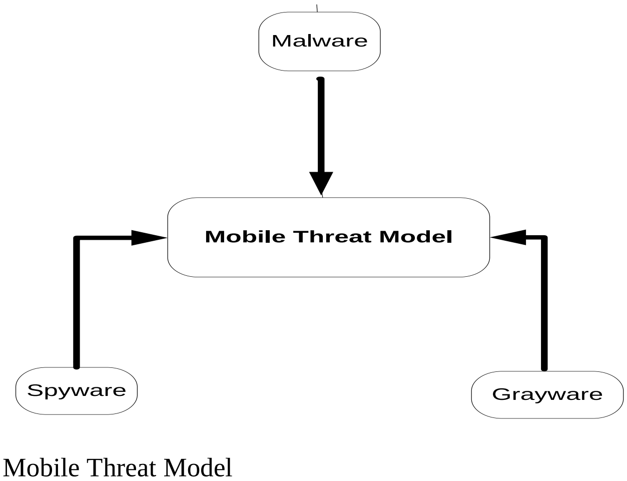

Figure 3: Mobile Threat Model

Malware gain unauthorized access to the device either by Drive-by download techniques like luring users to install an application or exploiting vulnerabilities in the system like flaws in SMS parser. Personal spyware collects personal information like location, contacts, call history etc. of a user. The attack is carried by gaining physical access to the device and installing the spyware. This attack is more targeted and the data collected is of interest to the person who installed it. Unlike malware, spyware does not send the data to the application developer. Grayware are applications that collect data to be used for marketing and user profiling. The intention behind grayware might not be to harm users. However, sometimes they may behave in a manner that is annoying or undesirable to users.

Mobile security threats could be physical, on network connectivity or a malware [35]. *Attack Vector* is a means by which an attacker can gain access to a system. [37], [35] categorized attacks to mobile devices into the following categories:

a. *Hardware Based*: These attacks are more related to physical access of the device such as intercepting mobile network operator smartcard communication. Removing SIM lock of the iPhone and man in the middle attack are some of the examples for hardware centric attack. Attacking the device via debugging functionality is also a type of hardware centric attack.
b. *Device independent attack*: Attacks that are independent of the device such as on infrastructure, protocols etc. come under this category. Global System for Mobile Communications (GSM) protocols were developed over 25 years ago and have lots of vulnerabilities like immature asymmetric crypto system, no network authentication to name a few. Similarly, there are a lot of flaws in SMS infrastructure like paging channel can overload the network. Flaws in MMS infrastructure causes the batteries to drain quickly.
c. *Software centric*: These attacks are based on exploiting the software running on the mobile devices for instance, Cabir malware propagated automatically on Symbian OS in 2004. Some of the software centric attacks uses:
   i. SMS communication channels
   ii. MMS communication channels
   iii. Attacks via mobile web browsers
   iv. Rootkit attacks
d. *User layer*: Attacks that are related to trick the user and not exploiting any technical vulnerability come under this category. Social engineering is a category to lure customers and perform attacks.

2.3.1 Malware Injection Attacks

Mobile cloud computing malware injection is the attack that attempts to inject a malicious service, application or even virtual machine into the cloud system depending on the cloud service model (SaaS, PaaS and SaaS) [32]. To perform this type of attack, an attacker is required to develop customized malicious application, service or virtual machine instance and then add it to the mobile cloud system. Once the malicious software has been added to the mobile cloud system, the attacker had to trick the cloud system to treat the malicious software as a valid instance or application. If it is successful, normal users are able to request the malicious service instance or application and then the malicious is executed.

Another scenario of this attack might be an attacker try to upload a virus or trojanized application to the mobile cloud system. Once the cloud system treats it as a valid service, the virus program is automatically executed and the cloud system gets infected by the virus which can cause damage to the cloud system [30]. In the event the virus damages the hardware of the cloud system, other cloud instances running on the same hardware may be affected by the virus program because they share the same hardware.

In addition, the attacker may aim to use a virus program to attack other users on the mobile cloud system. Once a client requests the malicious program instance, the cloud system sends the virus over to the client via the internet and then executes on the client's device. The client's device is then infected by the virus. The possible countermeasure for this type of attack could be performing a service instance integrity check for incoming requests [30]. A hash value can be used to store on the original service instance's image file and compare this value with the hash values of all new service instance images. As a result of using the hash values, an attacker is required to create a valid hash value comparison in order to trick the cloud system and inject a malicious instance into the cloud system. Other measures include the use of behavior-based malware detector that checks applications to be executed on devices without actually running the binaries or code. For already infected devices, the use of antivirus program becomes inevitable.

2.3.2 Flooding Attacks

Although data transmission between mobile clients and servers may be secure, attackers might choose to attack the cloud environment directly [30]. A common characteristic of the cloud system is to provide dynamically scalable resources with variability in usage benefit. Once there is more request from clients, the cloud system automatically scale up to meet the client's requirements by starting up new service instances. This can be a severe vulnerability for flooding attacks such as DoS which basically is an action of sending large number of meaningless requests to a certain service in the cloud system, once this happen, the cloud computing operating system realizes the extra requests and then begin to provide more service instances to support the workload. If the attacker continues to send more requests, the cloud system will try to work against the request by providing more computational resources. If this continues eventually, the system might consume all the resources on the cloud system which will then be not able to provide services to normal request from normal users.

Indirectly, other service instances on the same cloud system will be affected by the DoS attack. Once the resources of the server are depleted, there are no resources available for other services on the same server and consequently, other services might not be able to provide services to normal users. According to [30], DoS attack costs extra fees to the consumers. For example, Amozon Elastic Compute Cloud (Amazon EC2) charges customers based on actual data transfer [33]. Once a service instance running on Amazon EC2 has been attacked by DoS, the extra computational resources have been used and also there are a lot of additional data transfer between the attacker and the service instance. The service instance owner has to pay extra money to Amazon for the unexpected situation. Even though DoS attack may not be completely preventable, installing firewalls or Intrusion Detection System is able to filter malicious requests from attacking the servers.

2.3.3 Browser Security

It is a fact that clients are typically able to connect to mobile cloud computing via a web browser or web service hence, web service attack affects mobile cloud computing. XML signature element wrapping is a well-known attack for web service. Although web service security (WS-security) uses XML signature in order to protect an element's name, attributes and value from unauthorized parties, it is unable to protect the positions in the document [34]. An attacker is able to manipulate a SOAP message by copying the target element and inserting whatever value the attacker would like and moving the original element to somewhere else on the SOAP message [30]. In 2008, Amazon EC2 was discovered to be vulnerable to XML signature element wrapping attack [34]. A solution to this would be using a combination of WS-security with XML signature to sign a particular element and digital certificate such as X.509 issued by trusted certificate authorities. In addition, web services server side should create a list of elements that is used in the system and reject any message which contains unexpected messages from clients [30].

Furthermore, the interaction between clients and the cloud is via a web browser. The clients just sends request and then wait for the response from the server. Web browser is a common method to connect to the cloud system. Before a client can request for services on the cloud system, the client is requested to authenticate himself whether or not he has an authority to use the cloud system. From security point of view, web browsers rely heavily on SSL/TLS process. They are not able to apply WS-security concept (XML signature and XML Encryption) to the authentication process. Consequently, when a browser requests a service from the web service in the cloud system, it cannot use XML signature to sign the client's credentials like the username and password in order to authenticate the user and XML encryption to encrypt the SOAP message in order to protect data from unauthorized parties. The browser has to use SSL/TLS to encrypt the credential and use SSL/TLS 4-way handshake process in order to authenticate the client. Nevertheless, SSL/TLS only support point-to-point communications, implying that there is a middle tier between the client and the cloud server, such as a proxy server or firewall, the data has to be decrypted on the intermediary host.

If there is an attacher sniffing packages on that host, the attacher may gain the credentials and use the credentials in order to log in to the cloud system as a valid user. In addition, SSL/TLS has been broken by [34] in July 2009. Marlinspike used the technique called "Null Prefix Attack" to perform undetected man-in-the-middle attack against SSL/TLS implementation. This makes SSL/TLS a weak authentication for mobile cloud computing. Potential countermeasure [30] is that vendors creating web browsers should apply WS-security concept within their message level. As a result of this, web browsers are able to use XML encryption in order to provide end-to-end encryption in SOAP messages. Unlike point-to-point encryption, end-to-end encryption does not have to be decrypted at intermediary hosts. Consequently, attackers are unable to sniff and gain plain text of SOAP message at the intermediary hosts.

3.0 Conclusion

In this paper, selected mobile cloud computing security issues have been reviewd with possible countermeasures. It is quite obvious that mobile cloud computing security issues requires an in-depth analysis because attackers may choose to exploit cloud systems through various vulnerabilities. Attackers may target mobile cloud systems to perpetrate threats such as Eavesdropping (Snooping), Modification (Alteration), Masquerading (Spoofing), Repudiation, Denial of receipt, Delay, or Denial of service. These threats are achieved by the attacker through the use of any or combinations of the discussed threat model; malware, grayware and or spyware. Each of these threat models could be mitigated by appropriate countermeasures and security framework must target any or all the expected security goals for the relative security of the mobile cloud system.

REFERENCES

[1] Rashmi, A. Badjad, Monika Srivastava & Amit Sinha "Survey on Mobile Cloud Computing," International Journal of Engineering Sciences & Emerging Technologies,vol. 1, Issue 2, pp. 8 - 19, February 2012.

[2] Soeung-Kon Victor Ko, Jung-Hoon Lee, Sung Woo Kim, "Mobile Cloud Computing Security Considerations," Journal of Security Engineering, Vol. 9, No. 2, PP. 143-150, 2012.

[3] Khan A.N., Kiah M.L.M., Samee, U.K. & Sajjad A.M. "Towards Secure Mobile Cloud Computing: A Survey," Future Generation Computer Systems, pp. 1-22, 2012, DOI: 10.1016/j.future.2012.08.003.

[4] Niroshinie F., Seng W.L., & Wenny R. "Mobile Cloud Computing: A Survey," Elsevier; Future Generation Computer Systems, vol. 29, pp. 84 - 106, 2013. DOI: 10.1016/j.future.2012.05.023.

[5] Hoang T.D., Lee C., Niyato D. & Wang P., "A Survey of Mobile Cloud Computing: Architecture, Applications and Approaches." Wireless Communications and Mobile Computing, John Wiley & Sons Ltd., PP. 1-27, 2011. DOI: 10.1002/wcm.1203.

[6] Aubery-Derrick S., "Detection of Smart Phone Malware", Electronic and Information Technology University Berlin Unpublished PhD. Thesis. PP. 1-211, 2011.

[7] Department of Defence, "DoD dictionary of Military Terms," Available at http://www.dtic.mil/doctrine/jel/doddict/data/s/04767.html, 2001.

[8] Bishop M.A., "The Art and Science of Computer Security," Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2002.

[9] Richard Bejtlich, "The Tao of Network Security Monitoring: Beyond Intrusion Detection." Addison-Wesley Professional, 2004.

[10] National Institute of Standards and Computer Security Division Technology (NIST), "Information and Technology Laboratory. Standards for Security Categorization of Federal Information and Information Systems." Available at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf, February 2004. FIPS PUB 199, Visited 18.3.2012.

[11] U.S Code Section 3542: Definitions Title 44, Information Security. Visited 18.03.2012

[12] Eileen B., "Moving from Cloud Computing to Mobile Cloud Computing." Agilis Solutions, All about the Cloud, May 23-26, 2011.

[13] Roger C. (2011). "Mobile Cloud Adoption Challenges in the Enterprise,"Cloudcomputingtopics, April 16th, 2011. Available at http://cloudcomputingtopics.com/2012/04/mobile-cloud-adoption-challenges-in-the-enterprise/

[14] Zhangwei H., & Mingjun X. (2010). "Distributed Spatial Cloaking Protocol for Location Privacy," In Proceedings of the 2nd International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), 468, 2010.

[15] Sweeny L. (2002). "K-anonymity: A Model for Protecting Privacy." International Journal of Uncertainty Fuzziness and Knowledge-Based Systems, 10(5): 557-570, 2002.

[16] Wang S. & Wang X.S., "In-device Spatial Cloaking for Mobile Users Privacy Assisted by the Cloud." In Proceedings of the 11th International Conference on Mobile Data Management (MDM), 381, 2010.

[17] Chow C.Y., Mokbel M.F., & Aref W.G.C, "Query Processing for Location Services without Compromising Privacy," ACM Transaction on Database Systems (TODS), 34(4): 1-48, 2009.

[18] Deepti Sahu, Shipra Sharma, Vandana Dubey & Alpika Tripathi, "Cloud Computing in Mobile Applications," International Journal of Scientific and Research Publications, Vol. 2, Issue 8, PP. 1 - 9, August 2012.

[19] Peter S., "Challenges of Cloud Networking Security," Techreport, pp. 137-210, 2010. Available at http://www.hpl.hp.com/techreports/2010/HP-210-137.pdf

[20] Oberheide J., Veeraraghavan K., Cook E., Flinn J., & Jahanian F., "Virtualized In-cloud Security Services for Mobile Devices," In Proceedings of the 1st Workshop on Virtualization in Mobile Computing (Mobivirt), 31-35, 2008.

[21] Watson M.R., "Malware Detection in the Context of Cloud Computing." PGNet, PP. 1-5, 2012.

[22] Dazuko O.J., "An Open Solution to Facilitate On-access Scanning," In Proceedings of the 13th Virus Bulletin International Conference, 2003.

[23] Portokalidis G., Homburg P., Anagnostakis K., & Bos H. (2010). "Paranoid Android: Versatile Protection for Smart phones," In Proceedings of the 26th Annual Computer Security Application Conference (ACSAC), 347-356, 2010.

[24] Wang W., Li Z., Owens R., & Bhargava B., "Secure and Efficient Access to Outsourced Data," in ACM Cloud Computing Security Workshop (CCSW), PP. 55 – 66, 2009.

[25] Itani W., Kayssi A., & Chehab A., "Energy-efficient incremental integrity for securing storage in mobile cloud computing," International Conference on Energy Aware Computing (ICEAC), PP.1, January 2011.

[26] Song Z., Molina J., Lee S., Kotani S., & Masuoka R., "TrustCube: An Infrastructure that Builds Trust in Client," In Proceedings of the 1st International Conference on Future of Trust in Computing, 2009.

[27] Jakobsson M., Shi E., Golle P., & Chow R., "Implicit Authentication for Mobile Devices," in Processing of the 4th USENIX Workshop on Hot Topics in Security (HotSec), August 2009.

[28] Shi E., Niu Y., Jakobsson M., & Chow R., "Implicit Authentication through Learning User Behaviour," In Proceedings of the Implicit Authentication Security Conference (ISC), October 2010.

[29] Zou P., Wang C., Liu Z., & Bao D., "Phosphor: A Cloud-Based DRM Scheme with Sim Card," in Proceedings of the 12th International Asia-Pacific on Web Conference (APWEB), PP. 459, June 2010.

[30] Danish Jamil, "Security Issues in Cloud Computing and Countermeasures," International Journal of Engineering Science and Technology (IJEST), Vol. 3, No. 4, pp. 2672-2676, April 2001.

[31] Gruschka M. and Iacono L.L., "Vulnerable Cloud: SOAP Message Security Validation Revisted," IEEE International Conference on Web Service, pp. 631-635, July 2009.

[32] Abah Joshua, Francisca N. Ogwueleka "Cloud Computing with Related Enabling Technologies" International Journal of Cloud Computing and Services Science (IJ-CLOSER), vol. 2, No. 1, pp. 40 – 49, February 2013.

[33] Amazon Web Service, (2009). Amazon Elastic Compute Cloud. Available at http://aws.amazon .com/ec2

[34] Marlinspike M., "Null Prefix Attack against SSL/TLS Certificates," 2009. Available at http://www.thought crime.org/papers/null-prefix-attacks.pdf

[35] Srikanth Ramu, (2012), "Mobile Malware Evolution, Detection and Defense" Term Survey Paper, Institute for Computing, Information and Cognitive Systems, University of British Columbia, Vancouver, Canada

[36] Adrienne P.F., Matthew F., Erika C., Steve H. & David W. (2011). "A Survey of Mobile Malware in the Wild", Proceedings of the 1st ACM Workshop on Security and Privacy in Smart phones and Mobile Devices, October 17-17, 2011, Chicago, Illinois, USA.

[37] Becher, M., Freiling F.C., Hoffmann J., Holz T., Uellenbeck S., Wolf C. (2011). "Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices," Security and Privacy (SP), 2011 IEEE Symposium, Vol., No., PP.96-111, 22-25 May 2011.

BIBLIOGRAPHY OF AUTHORS

)	Victor Onomza Waziri obtained his BSc/Ed (Maths) from Usmanu Danfodiyo University Sokoto (1990), M. Tech (Applied Mathematics) and PhD (Applied Mathematics) based-on Computational Optimization in 1998 and 2004 respectively From the Federal University of Technology, Minna-Nigeria. He did his PostDoctoral Fellowship in Computer Science at the University of Zululand, South Africa in 2007. He is the Current Head of Cyber Security Science, Federal University of Technology, Minna-Nigeria. His research works are in the fields of Computational Optimization, Modern Cryptography, CyberSecurity/ Malware Detection, Mobile Cloud Computing Security, Programming and Network Security. He has published many academic papers at both local and International Scene Victoor.waziri@futminna.edu.ng/ onomzavictor@gmail.com
	Joshua Abah received a B.Tech (Hons) in Computer Science from Abubakar Tafawa Balewa University Bauchi, Nigeria in 2005, and MSc. in Computer Science from Bayero University Kano, Nigeria in 2011. He is at present a Ph.D fellow in Computer Science at the Federal University of Technology Minna, Nigeria. He is currently working in the academia where he has been for the past seven years. His research interests include Mobile Cloud Computing Security, Network Security, Cloud Computing, Virtualization, Scheduling Algorithms, QoS and Computer Education. He has well over eight journals both local and international and has authored five textbooks to his credit.
Thirth author's photo(3x4cm)	Prof. Olumide Sunday Adewale, is a Professor of Computer Science. He lectures at the Federal University, Akure-Nigeria. Has published many academic papers at both local and at International Scene. He is a Visiting Professor to the Department of Computer Science, Federal

	University of Technology, Minna-Nigeria.
	Muhammad Bashir Abdullahi received B.Tech (Honors) in Mathematics/Computer Science from Federal University of Technology, Minna-Nigeria and Ph.D. in Computer Science and Technology from Central South University, Changsha, Hunan, P. R. China. His current research interests include trust, security and privacy issues in wireless sensor and ad hoc networks, Internet of things and information and communication security. Email: el.bashir02@futminna.edu.ng