International Journal of Advance Research, IJOAR .org
Volume 3, Issue 3, March 2015, Online: ISSN 2320-9194

SECURITY ISSUES IN MOBILE CLOUD (PLATFORM RELIABILITY, DATA PRIVACY AND PROTECTION)

Rida Ghafoor Hussain, Muhammad Fahad Khan
Department of Software Engineering
University Of Engineering And Technology, Taxila, Pakistan.
rida_ghafoor@yahoo.com, itsfahad786@hotmail.com

KeyWords
CMA, PaaS, IaaS, SaaS, malware, CS, NS, manifest file, VPN technology.

ABSTRACT

In the last few decades, the computation and technology has substituted from client-server to web-based systems. Recently we are recouping to internet-based technology "Cloud Computing" which is virtually centralized. Cloud Computing is an emanate archetype for wide-ranging infrastructures. It reduces the overall cost by providing an on-demand mechanism based on shared computing and stored resources. The methodology relies on pay-per-use business model. Cloud computing has also significantly boost the computing facility of mobile devices. With the cloud methodology, mobile users are capable of performing major computational operations such as multimedia processing, searching and data mining. With the fleet growth of cloud computing in mobile industry, notably with the development of smart phones , many new mobile security issues have arise . In this paper we will discuss security issues in mobile cloud including platform reliability, data privacy and protection. Some solutions to related issues are also proposed.

Introduction:

In the current years, the explore center for both academic world and business is cloud computing. Cloud computing offers a sequence of services such as IaaS (Infrastructure-as-a-Service), SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service) etc by means of extensibility and demanding services. So, it is known as a new epoch of information technology. To relish on-demand high aspect utilization and business from a mutual pool of configurable computing chattels , data owners can casually stock their data in the cloud . In the last few years, cloud computing has developed from being a propitious dealing notion to one of the greatest rising segments of the IT business. Those cliquish practices and services based on cloud computing are considerably emerging. Cloud computing is the highly hallucinate perception of computing as a service. In the meantime, with the swift progress of cellular phone network and haulable terminals, smart phones are more and more preferential by users. It is becoming a tendency to use cellular terminals to approach the services provided by the cloud. Therefore mobile cloud computing is developed out of the raised intense technologies: cloud computing and mobility [1]. According to the analysis from Allied Business Intelligence, more than 2.4 billion users will use the cell phones to access the cloud computing service by 2015. And more than a few enterprises have presented classical mobile cloud products. For example, Google presents some cloud-based products for end users and firms. The key innovation amid them is the Android operating system for cellular phones. Further Google has lofted novel appliance based on cellular terminal and cloud computing, e.g. Google Maps, streets and topographical explore. Formerly, Microsoft had proposed a program called the LiveMesh, which can incorporate a few MAC-based Apple computers, desktops operating windows operating system and smart phones running windows mobile system. In the intervening time , LiveMesh is a technology including software practice by which users can approach and share their information and appliances. Based on the abstraction of cloud computing, mobile cloud computing is construed as a representation for providing various IT basics and data maintenance over the mobile network by means of appealed self-service. Mobile cloud computing is the utilization of cloud computing in consolidation with mobile devices [2]. There are several confrontations to be solved. Among these are security and privacy issues, since the user's info has to be broadcast to the Cloud and thus evacuate the security-orbit of the data owner. The measures include the device security of the client side termination, the risks of websites, the findings, identification and observation of interventions, the protection and access of repository in the cloud side, the exposure of system leakage and the examination of real-time fixing process, the running of server structure and cellular e-commerce processing, and the co-ordinated investigation of linked protection information and concerns. Finally, a data security format with unrestricted scrutinizing plan is marked that will concentrate on a figure of these aspects, by providing a means to permit for information to be encoded in the Cloud without failure of convenience or service for certified enterprises. This proposal is not essentially a substitute for conventional solitude and secracy dealings for data, but somewhat an enrichment which offers users, at moreover the personage or project level,a greater scale of assurance in the approval of inventive, cost-saving Cloud computing mechanisms.

Literature Review:

Security risks against the Cloud, the mobile devices, services and practices on these devices which can be indigenous or mobile web practices are the cause of security concerns in Mobile Cloud Computing. Mobile cloud applications depict client private information to distinct security risks. In the mobile cloud background, information and application are lay up in cloud servers that hoist the safety issues for the users of mobile computing. This argument is a key obstacle in the improvement of this novel technology [3]. In allpurpose, we can organize cloud security services in two types: Critical Security (CS) service and Normal Security (NS) service. The CS service generally employs additional cloud computing resources; though it generates more rewards to the cloud provider since the CS service clients require to compensate extra for using the CS service.CS service provides well-built security defense such as by means of longer key size, severe security approach tactics, seclusion for protecting data, and so on. With the raise of the figure of CS and NS service users, it is imperative to distribute the cloud resource to enlarge the system rewards with the application of the cloud resource utilization and interests produced from cloud users. [4]. Malware detection on phones, comparatively, is not only a tedious assignment, but also one that consume much of their enhanced efficiencies. So one of the major crisis now in front of us is, what we can do to conserve and protect our natural scarce each day acquaintance [5]. Running more cellular applications and services will augment the intimidation of malware that can be installed in the smart phones and then make vulnerable the significant data handled in the phones. Furthermore, the system complication of wireless devices is decreased by running effortless and reliable software, and consequently the possibility of being adjusted is also minimized [6]. Daniela POPA, Marcel CREMENE, Monica BORDA, Karima BOUDAOUD [7] in "A Security Framework for Mobile Cloud Applications" have proposed a framework to protect the data transmitted between the elements of the same mobile cloud application, also this mechanism takes into concern the user predilections and the mobile device practices. The previous researches [8] [9] on mobile security risks have declared the following types of mobile intrusions: physical based ,application based , network based and web-based interventions. Consequently, data may be degraded, customized or removed and the application practices can be changed. Repackaging was the most used procedure in 2011 to contaminate services and applications running under Android [8]. An invader takes a well function; changes it so that this carries malicious code and after republishes it. The agenda provides: a function whose characteristic is to examine the various contact levels listed in "manifest" file and to estimate the threats for the access approved by client. The most significant aspects of this structure is that: 1) the user priorities are taken into deliberation . 2) it permits applying various security acuities to different kinds of information and not the same acuities to all the data processed by the application 3) the mobile device practices (e.g. energy consumption) are also taken into description. The outline provides also a resolution to confirm the reliability of an application. Hui Suo, Zhuohua Liu, Jiaf Wan, Keliang Zhou [10] in "Security and Privacy in Mobile Cloud Computing" have outlined security and privacy

conflicts from three layers, which are mobile cloud, mobile network and mobile terminal. Then, according to the risks we gave the present ways such as anti-malware, privacy protection, key management and encryption, access control . Cloud AV ,an anti-malware provides several important benefits as follows: improved detection of malicious software; erasing the impact of antivirus accountabilities; showing detection of beforehand affected hosts; improved argumentation efficiencies; better organize skill and association. Improving the security consciousness of the clients is the major area to avoid the malware. For instance, don't get on the mysterious links; be cautious of getting the data communication from unfamiliar phone; avoid install new illegal software; power cut the interface of Bluetooth or Wi-Fi etc. so that the communication option of the malware will be abridged. To put off delicate information from leaking, the information should be reserved in cipher text in the cloud. The modern research on the cipher text processing is the privacy homomorphism algorithm. Gustavo de los Reyes, Sanjay Macwan, Deepak Chawla, Cristina Serban [11] in "Securing the Mobile Enterprise with Network-Based Security and Cloud Computing " effectively handles the Advanced Persistent Threats (APT) and attacks and proposed enhanced architecture - the Virtual Private Gateway for end devices. With the VPG, end devices always have a VPN (Virtual Private Network) between any of their endpoints (mobile phones, laptops, or PCs) and the VPG4.In addition, there is a VPN (either IPSec or MPLS) between the VPG and the Cloud. Therefore, all transmissions between the endpoints and the Cloud are consistently secured, and well grained procedures can be simply functional to both inflowing and outflowing interchange. ZHOU Lian-chi, XIU Chun-di [12] in" Cloud Security Service Providing Schemes Based on Mobile Internet Framework" focuses on giving the energetic contrasting cloud security practices cellular internet infrastructure. By taking into account the issues of access power, on-demand practice and flexible modification, this research suggests the subsequent three practical sub-schemes correspondingly: a cloud service access control model which helps the authorization changes, a security self-adaptive means for cloud service and a cloud security service adapting structural design for distinctive security needs. These schemes can help understand the controllability, modifiability and adjustability of the cloud security practices. Yu-Jia Chen and Li-Chun Wang [13] in "A Security Framework of Group Location-Based Mobile Applications in Cloud Computing" analyze the security problems of LBS in cloud computing, they implemented a location-based set development service called JOIN [14], The most important thought of JOIN is to collect the information of your acquaintances close by and propose some attractive activities near your recent site. Additionally, clients can simply perform an opinion poll for the optional activities. The proposed schema initially recommend IMSI-based JOIN secure (IJS) algorithm that use international mobile subscriber identity (IMSI) as user identification incorporated with encryption algorithms.. The focal plan of the planned IJS algorithm is to employ encrypted IMSI to conceal users' accurate status with distributed storage. The IJS algorithm improves isolation, authentication, and stability. Saeid Abolfazli, Zohreh Sanaei, Ejaz Ahmed, Abdullah Gani, Rajkumar Buyya, [15] in "Cloud-Based Augmentation for Mobile Devices: Motivation, Taxonomies, and Open Challenges" have briefly described deficiencies of present cellular devices as an incentive for expansion. Cloud resources in this area are manifested as remote static clouds, immediate mobile and stationary computing entities, and hybrid arrangement of resources. CMA (cloud-based mobile augmentation) procedures not only improve processing, energy, and storage efficiencies of smart phones, but also modify data security and protection, data ubiquity, convenience, and user view while using distributed application programming.

Methodology:

The mobile terminal ahs the following characteristics: third party software , open operating system, wireless access. With the benefits of mobile cloud computing, it has some privacy and security issues as well. Mobile cloud applications expose user data to applications that run on mobile devices or cloud. The last studies [16][17] on mobile security issues revealed that applications, websites, network based attacks affect the integrity and confidentiality of mobile data and applications. The data in this way can be corrupted , deleted or the functionality of any mobile app can be altered.

Repackaging was the technique used to infect android applications in 2011 [16]. The suspicious attack alters the healthy applications by malicious code and republishes it. Similarly, cloud can be targeted concerning data privacy, data ownership and location and communication channel can be the target of malicious attacks.

The data between devices and cloud travels over the internet and is stored in multiple locations. Similarly, cloud providers deals with multiple customers at a time which may raise level of exposure to possible breeches accidently or deliberately. The security aspects involves issues regarding data security, location privacy, risk management, identity privacy and authentication, malware and software vulnerabilities. Privacy is not a barrier, it must be taken into consideration.

Security Design of Cloud Computing:

The mobile cloud application providers have to secure data and ensure privacy. The design is based on privacy such that it aims to prevent privacy infarctions rather than waiting for privacy risks to materialize and taking remedies and resolving issues. Therefore, Privacy by Design comes before-the-fact, not after. The architecture requires collaboration between agents (consumer and requestor) and service providers (the Cloud access control service provider (ACSP) [18] and the Cloud data service provider (DSP)).

In Fig1 : if requestor wants to access consumer's data, it contacts the ACSP for authorization purpose. Once authenticated, Cloud ACSP allows access to the requestor. The authorization message comprises of three components: a decryption key for released data, the subset of data to be released and a notification to cloud DSP that requestor has been authenticated. An identity management is maintained allowing consumers the option of secure interaction. It also ensures that information is not leaked into the Cloud through data access patterns.

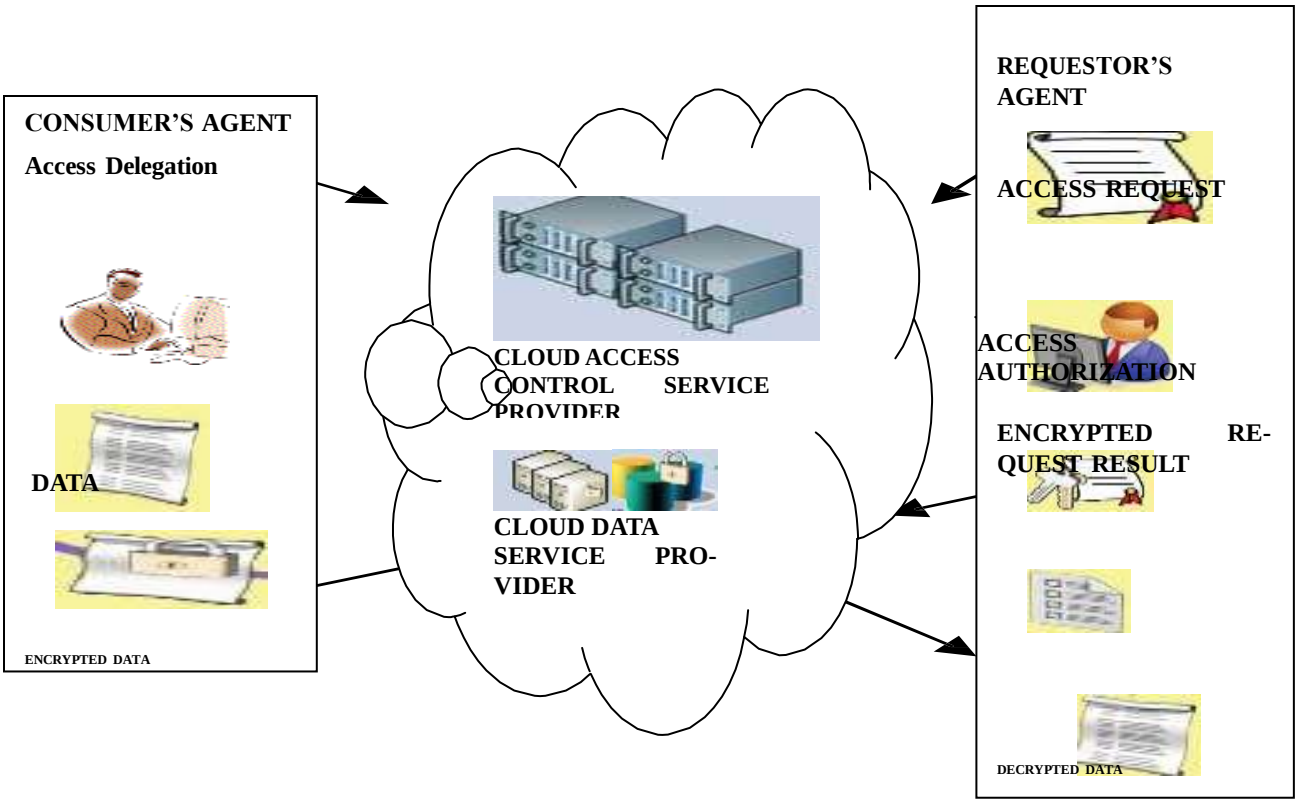

Fig. 1: Privacy Preserving Cloud Computing Architecture

SECURITY AND PRIVACY ISSUES IN MOBILE CLOUD

1) Malware:

Malware is the most common issue due to openness and versatility of mobile terminals. Some malware can be automatically down-loaded with other software and applications unknown to users . By this means, it gets illegal access to the private information and users suffer information leakage and privacy issues. The malware can be spread among mobile network via 3G network, Bluetooth, mms attachments and USB interface. For prevention from malware, antivirus for mobile terminals have been developed.

2) Software Vulnerabilities:

Smart phones now a days are widely used . Users often handles data through file transfer for which FTP (File Transfer Protocol) is usually applied .The username and password are transferred over the network and saved in a configuration file. This causes illegal access, deletion and malicious attack to the smart phone data .

3) Mobile Users:

Users are mostly unaware of security measure, they misoperate mobiles , installing irrelevant software and clicking unwanted links ,resulting in privacy leakage and information loss. Application integrity has to be verified at installation and update.

4) Mobile Network Security :

Broad access ways are responsible for more security threats and attacks. Public places offers public wifi, people often use internet via Smartphone at such places which is also risky causing potential information leakage. Even the private wifi also causes security threats as encryption mechanism is risky. The interaction between mobile devices and cloud service providers is frequent through different interfaces, which is also dangerous.

5) Threat to Platform Reliability:

The cloud platform is susceptible to malicious attacks because of information resources of users. The attackers steal valuable infor-mation and services. For example, when users deliver all their data to the cloud without any backup or disaster recovery, risk is high for loss of data.

The user data is stored randomly all over the world in cloud infrastructure and users themselves don't know the exact location, this is also increased risk to exposure.

SECURITY MEASURES FOR MOBILE CLOUD COMPUTING:

By taking into consideration network access, privacy protection, encryption, key management , access control we can assure security and privacy in cloud computing to an extent.

1) Anti-malware:

When a malware is detected at the cloud side, legal software can be run to remove it. From legal, we means authenticated and ac-crediated without harming the files when removing malware. The other is prevention of mobile devices from malware through user

care which will be discussed later.

2) Protection Against Software Vulnerabilities:

Users should be careful while downloading third party software. They should pay attention on timely installations of patches or revamped versions from research and development company of the operating system. For example, checking software legitimacy and integrity is important procedure before installation of software.

3) Application Integrity:

For checking integrity of applications, the following verifications should be accomplished:

1) the existence of application

2) the application signature

3) the application access into the "manifest" file.

For verification of an application, the name is searched in official application store (e.g. Amazon, Apple) and the signature is compared. If its different, it is malicious else it is reliable.

4) Regulating Users' Behavior:

Users should be careful while using wifi, Bluetooth etc on their devices. For example, shut down interface of Bluetooth and wifi etc so that malware transmission will be reduced. Similarly, improving security awareness like avoid clicking the unexplained links and careful in receiving data transmission from strange phone and so on.

5) Protection to Platform Reliability:

Cloud providers should offer complete backup and recovery solutions to users data. They should integrate current security technologies including VPN technology, encryption, authentication and access control.

6) Data Encryption and Key Management:

The sensitive data need encryption technology in survival period from storage to transmission. The data should be stored in cipher text format. Encryption reduces the utilization rate of data. Similarly, key management is another hot topic in securing data.

7) Authentication and Access Control:

The authentication management system for securing cloud computing refers to identity of users. Users are identified in two ways. The user is identified through identifiers, and a user can be allowed to have multiple identifiers. The other type of identification is through habits and behaviors such as memorized data, their belongings.

Similarly, after transmitting data, access is provided in two ways. The users are pre-assign access permissions through Access Control List (ACL) mechanism [19, 20] and the other type is access permission to the account level, all tenants share their delegated account.

8) Privacy Protection:

The governments from all over the world have developed protection plans and strategy. For example, British government introduced Data Protection Act in 1998, the European Union issued data protection directive in 1995 and so on. Similarly, technologies have also played important role in privacy protection. P3P (Platform for Privacy Preferences), announced by WWW consortium is under use of 40% of the top 100 global internet sites. To sum it up, the current approaches on security and privacy of mobile cloud computing are shown in Table I.

TABLE I. SECURITY ISSUES AND CORRESPONDING CURRENT APPROACHES

Security issues		**Current approaches**
Mobile terminal	Malware software	Detection and prevention
	Software vulnerabilities (application software; operating system)	Installing the system patches Checking the software legitimacy and integrity
	Others(lack of security awareness, mis-operation)	Regulating the users' behavior
Mobile network	Information leakage or Malicious attack	Data encryption
	Platform reliability	Security protocol
Mobile cloud	Data and privacy protection	Integrating the current security technologies; Key management and data encryption; Authentication and access control Privacy and data protection

Conclusion

In this research work, initially a security design for mobile cloud computing is proposed.The design is based on privacy such that it aims to prevent privacy infarctions rather than waiting for privacy risks to materialize and taking remedies and resolving issues. Similarly, security and privacy issues in mobile cloud computing are discussed like network security, platform reliability and software vulnerabilities. The research is further concluded with security measures for protection, data encryption, key management and platform reliability.

References

[1] CSA(c1oud security alliance), "Security guidance for critical areas of focus in cloud computing," http://www.cloudsecurityalliance.org/ guidance/csaguide.v3.0.pdf,2011.

[2] W. Song and X. Su, " Review of mobile cloud computing," in Proc. of 2011 IEEE 3rd International Conf on Communication Sofware and Networks (ICCSN), May 2011, pp. 1-4.

[3] Mojtaba Alizadeh, Wan Haslina Hassan "Challenges and Opportunities of Mobile Cloud Computing" 978-1-4673-2480-9/13/$31.00 ©2013 IEEE

[4] Hongbin Liang,Dijiang Huang,LinX.Cai, Xuemin (Sherman) Shen, Daiyuan Peng "Resource Allocation for Security Servicesin Mobile Cloud Computing" in IEEE INFOCOM 2011 Workshop on M2MCN-2011, 978-1-4577-0248-8/11/$26.00 ©2011 IEEE

[5] Xuesen Lin "Survey on Cloud Based Mobile Security and A New Framework for Improvement " in proceeding of the IEEE International Conference on Information and Automation Shenzhen, China June 2011, 978-1-61284-4577-0270-9/11/$26.00 ©2011 IEEE.

[6] Dijiang Huang, Xinwen Zhang, Myong Kang, Jim Luo "MobiCloud: Building Secure Cloud Framework for Mobile Computing And Communication" in 2010 Fifth IEEE International Symposium on Service Oriented System Engineering, 978-0-7695-4081-8/10 $26.00 © 2010 IEEE DOI 10.1109/SOSE.2010.20

[7] Daniela POPA, Marcel CREMENE, Monica BORDA, Karima BOUDAOUD "A Security Framework for Mobile Cloud Applications", European Social Fund through the Sectorial Operational Program Human Resources 2007-2013.

[8] Lookout Mobile Security, "Lookout Mobile Threat Report", August 2011.

[9] C. Nachenberg, "A Window Into Mobile Device Security – Examining the security approaches employed in Apple's iOS and Google's Android", Symantec Security Response.

[10] Hui Suo, Zhuohua Liu, Jiaf Wan, Keliang Zhou "Security and Privacy in Mobile Cloud Computing" 978-1-4673-2480-9/13/$31.00 ©2013 IEEE

[11] Gustavo de los Reyes, Sanjay Macwan, Deepak Chawla, Cristina Serban "Securing the Mobile Enterprise with Network-Based Security and Cloud Computing " 978-1-4673-1466-4/12/$31.00©2012 Crown

[12] ZHOU Lian-chi, XIU Chun-di," Cloud Security Service Providing Schemes Based on Mobile Internet Framework" in 2012 International Conference on Computer Science and Electronics Engineering ,978-0-7695-4647-6/12 $26.00 © 2012 IEEE DOI 10.1109/ICCSEE.2012.184

[13] Yu-Jia Chen and Li-Chun Wang "A Security Framework of Group Location-Based Mobile Applications in Cloud Computing"in 2011 International Conference on Parallel Processing Workshops, 1530-2016/11 $26.00 © 2011 IEEE DOI 10.1109/ICPPW.2011.6

[14] Y.T.Lee, L.C.Wang, and R.H.Gau, "Implementation Issues of Location-Based Group Scheduling for Cloud Applications," in IEEE VTS Asia Pacific Wireless Communications Symposium Conference (APWCS 2010), May 2010.

[15] Saeid Abolfazli, Zohreh Sanaei, Ejaz Ahmed, Abdullah Gani, Rajkumar Buyya, "Cloud-Based Augmentation for Mobile Devices:Motivation, Taxonomies, and Open Challenges" in IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION

[16] Lookout Mobile Security, "Lookout Mobile Threat Report", August 2011.

[17] C. Nachenberg, "A Window Into Mobile Device Security – Examining the security approaches employed in Apple's iOS and Google's Android", Symantec Security Response.

[18] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in *Proc. of ESORICS'09*, Saint Malo, France, Sep. 2009.

[19] X. Tianyi, H. Dijiang, M. Deep and A. Shingo, "MobiCloud: a Geo-distributed mobile cloud computing platform," in Proc. of 8th International Conf. on Network and Service Management (CNSM), 2012.

[20] H. Takabi, B. James and D. JosHi, "Security and privacy challenges in cloud computing environments,