



A Survey of Mobile Cloud Computing: Secure Channels Transmission in Mobile Cloud Computing

Riyadh R. Nuiaa

Ammar Awad Kazm

Wasit University

Wasit University

Abstract

Mobile cloud is the infrastructure that facilitates the offloading of storage and computing resources of mobile devices pertaining mobile applications to cloud computing. Mobile devices can run expensive applications using mobile cloud as they can outsource services to cloud while providing interface for mobile users. Emerging mobile applications that are expensive can overcome the inherent problems of hand held devices through the concept of mobile cloud computing. The offloading process provide mobiles a rich platform for pervasive computing with on-demand services linked to cloud computing through mobile cloud infrastructure. Thus the mobile cloud computing is an inevitable phenomenon which bring about plethora of pros besides the mobility. The mobile cloud users can perform their resource intensive operations on the fly without time and geographical restrictions. In spite of the advantages it bestows mobile cloud computing has its own security issues. This paper throws light into the security issues and solutions in terms of secure channels transmission in mobile cloud computing. In this paper, we present state-of-the-art of mobile cloud computing besides its security aspects that are to be taken care of for successful mobile cloud computing.

Index Terms – Cloud computing, mobile cloud computing, security, offloading services



I. INTRODUCTION

Mobile computing is becoming increasingly popular because people of all walks of life use smart phones and most of them use applications that are Internet aware. According to Juniper Research cloud-based mobile applications can cause enterprise and consumer market to rise up to \$9.5 billion by 2014 [1]. In the recent past people started preferring mobile applications. Applications pertaining to new, travel, social networking, business, health and games are some of the examples that run in mobiles. This has paved way for mobile application download centres like Ovi suite, iTunes and so on. The reason behind the usage of mobile applications in abundance is that they bring about convenience and users are happy as they can use them in transit achieving location independence. Without time and geographical restrictions and without moving places right from the current place people are able to get connected to the world with mobile applications. Thus mobility become significant characteristics in pervasive computing.

Though mobility has plethora of benefits, it brings with it inherent problems like low connectivity, finite energy, and scarcity of resources [2]. The future applications are supposed to provide real time response to queries from human users and also sensors. High level of response is expected from real time applications that need intensive computing resources. There are some mobile applications that are meant for providing location based services and social networking. There is an extensive usage of sensor devices in the real world for getting GPS reading which is actually expensive besides degradation of services. Moreover there are applications that need high level of processing such as wearable computing, augmented reality, natural language processing, speech synthesis and video games that demand high computing resources. As these trends are emerging in mobile applications, it is essential to think about the feasibility of the mobile computing considering its inherent limitations pertaining to resources.

In the recent past the problem described above was addressed using cloud computing. Cloud computing is a new model of computing that facilitates sharing of resources from a pool of resources through Internet [3]. With cloud computing all services are provided by cloud and its data centres while the applications might run in mobile devices. It does mean that the processing and storage services which are very expensive in the latest trendy



applications are outsourced to cloud. Cloud computing is also known as utility computing or on-demand computing where the computational resources are provided in pay per use fashion.

Therefore the users of cloud or organizations that use cloud need not invest in computing resources. Instead they use and pay as they use. The cloud services include software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) [4]. Extensive surveys on cloud computing [5], [6] and [7] can provide necessary information on advantages and potential challenges of mobile cloud computing. Typical infrastructure in mobile cloud computing is shown in Figure 1.

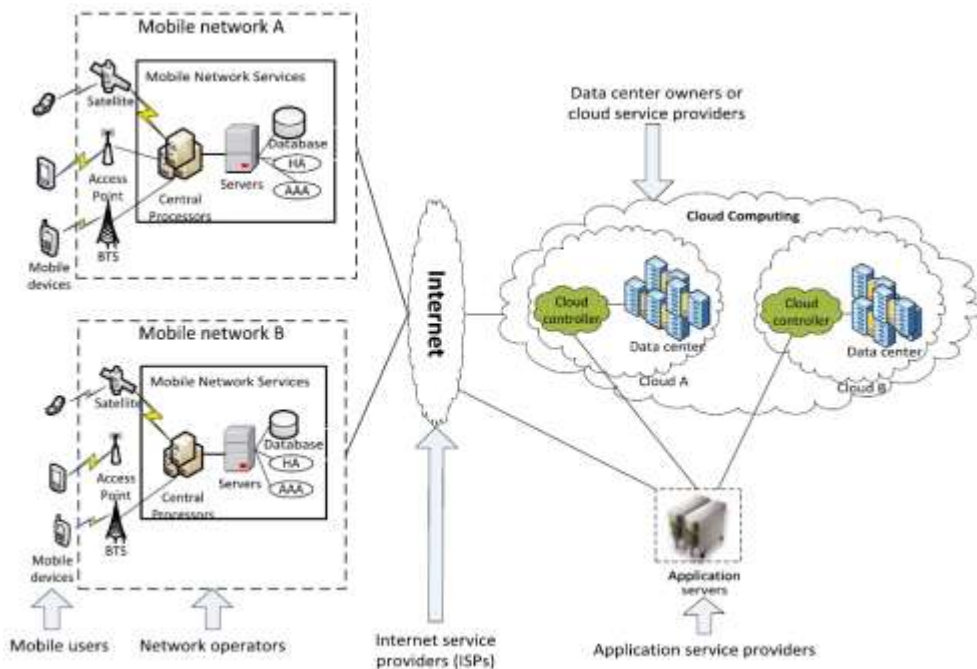


Figure 1 – Architectural overview of mobile cloud computing [8]

As shown in Figure 1, it is evident that the mobile networks are communicating with cloud computing resources or services through Internet. The mobile devices which are in mobile networks offload their storage and computing services to cloud so as to form a mobile cloud environment. The



nodes in the mobile network act as service nodes though they delegate actual service to cloud.

Mobile cloud computing is the concept in which mobile applications can offload data and computations to cloud computing in order to address the problems associated with modern applications as described earlier. The infrastructure that includes the mobile devices and the data storage and processing facilities to which offloading data and computations is done is known as mobile cloud. By exploiting the mobile cloud the resource intensive applications that are to run in the mobile devices can be offloaded in terms of storage and processing. However, it is essential to understand the main difference between the mobile cloud computing and cloud computing. In this paper we provide present state-of-the-art of mobile cloud computing and secure channels transmission in mobile computing.

Our contributions in this paper include the review of useful information regarding mobile cloud computing, its differences from cloud computing, the offloading process and secure channels transmission in mobile computing. This paper also throws light into the potential issues in the security of mobile cloud computing besides possible solutions. The remainder of the paper is structured as follows. Section 1 provides the introductions. Section 2 provides the motivation. Section 3 provides information on security issues in mobile cloud computing. Section 4 throws light into secure channel transmission in mobile cloud computing. Section 5 concludes the paper besides providing directions for future work.

II. Motivation

This section provides information pertaining to mobile cloud computing and why the world is forced to have it besides alarming security issues. Mobile cloud computing is the technology that enables mobile devices to participate resource intensive applications as they can offload the services like storage and computing to cloud computing. The infrastructure that makes this phenomenon possible is known as mobile cloud [1]. The computing which takes place through the mobile cloud is known as mobile cloud computing. Mobile cloud computing is essential as people of all walks of life started using mobile devices and they like to perform most of the operations through mobile devices. This has forced to have mobile cloud computing platform



which serves the mobile users to have on-demand, resource intensive applications. Mobile devices act as service nodes [1]. Modern computing devices brought about the dream of pervasive computing to be a reality [2].

III. SECURITY ISSUES IN MOBILE CLOUD COMPUTING

There are many security issues with mobile cloud computing as the mobile networks provide heterogeneous environment and the nodes in mobile network exhibit mobility [1]. With mobile cloud computing, the users of the data do not have control over it. Therefore users are concerned about privacy and security of the outsourced data. Moreover the collaboration between public cloud and also mobile cloud provides other security challenges and performance issues [2]. There are security issues in mobile cloud computing in terms of authentication, VIRUL, and malicious code detection. Therefore security as a service is required in mobile cloud computing [8]. Security threats are inherited from conventional cloud computing as the mobile devices work in collaboration with it. Mobile cloud computing also inherits security vulnerabilities from the underlying mobile network [9]. Information security is another issue as the offloaded data travels through Internet and resides in service provider's storage facilities. Such data is not under control of the owner of data. The data resides in an untrusted environment [10].

User's location data in cloud database is not protected. This could lead to vulnerabilities as adversaries can take it as an advantage [4]. Impersonating mobile user is an important security issue in mobile cloud computing as explored by Khan *et al.* [5]. Security in mobile cloud computing has to be given paramount importance as billions of devices are connected to Internet and most of them are involved in cloud computing [7]. There are privacy sensitive applications that can run in mobile cloud. Especially location based services are vulnerable to privacy and security challenges where confidentiality needs to be managed [11]. According to Bourouis *et al.* [12] security key exchange is one of the challenges to be addressed in mobile cloud computing. Rolim *et al.* [13] opined that mobile cloud will have seamless integration with other cloud platforms that are nothing but third party infrastructure that is essentially untrusted [14] and [15]. Since the modern mobile devices are running applications that are executed by PCs, it is essential to ensure that the conventional security mechanisms are tailored and employed in mobile cloud for security [14]. Despite the advantages of



mobile cloud computing, it has security issues and as such security has to be given paramount importance [16] and [17].

Smart phones and other small hand held devices which are Internet-aware can participate in mobile cloud computing. However, they exhibit plethora of security vulnerabilities as they do not have sufficient resources and they have mobility [17]. Moreover manufacturers of mobile devices do not focus providing sufficient security [18] and [19]. As devices involved in mobile cloud computing are at different geographical locations in distributed environment, the end to end secure communications is challenging issue to be addressed [19],[20] and [21]. Information security in cloud computing and mobile cloud computing is to be given highest importance and this process is never ending process that needs to adapt to changing security requirements of IT systems [22] and [23]. As explored in [24] the specific security risks in cloud computing include security loop holes in cloud infrastructure, sharing technical flaws, insecure interface API, nefarious use of cloud, VM level attacks, lack of browser security, issues with XML signatures, user access privileges, malicious insiders, service hijacking, flooding attack, internet protocol vulnerabilities, mis-configuration of network security, network attacks, and lack of safety standards. Security needs to be provided as a service in mobile cloud computing so as to standardise the counter measures that can benefit all mobile cloud users [25].

IV. Prior Works on Secure Channel Transmission in Mobile Cloud Computing

As understood from the previous section, it is crystal clear that security threats in cloud computing prohibit the rapid adaptation of mobile cloud computing. This section reviews the present state-of-the-art of the solutions that can provide secure communications in mobile cloud computing.

1- MobiCloud

Huang *et al.* [1] proposed an architecture named MobiCloud for mobile cloud computing to take place in a secure environment. The MobiCloud reference model makes use of traditional computing services besides specifying security mechanisms. It considers the mobile nodes as service nodes in mobile cloud. The communication in the mobile cloud is enhanced by



employing mechanisms like risk management, secure routing, and trust management. At MANET level the framework takes care of trust management, localization, routing, and information dissemination. It also has provision for virtualization of MANET operations to leverage performance. The trust model adapted by MobiCloud includes access policy enforcement, key management, and identity management. Communication and performance metrics are employed to ensure that the risk assessment is possible. The data generated by MobiCloud can be studied to know security issues and how the framework responded towards getting rid of such risks. MobiCloud protects information of mobile users by isolating security. Effective intrusion detection and response mechanisms are in place in MobiCloud. It also has provision for rendering service compositions and applications to the devices in the underlying MANET.

Damage recovery is possible with MobiCloud as it stores data in a secure place and the lost data can be restored. MobiCloud maintains information repository that can be used to handle unpredictable situations. Fine-grained mechanisms are in place for security and resource isolation. Monitoring service, on-demand service and advising service provide features for prediction, controlling and post-event analysis respectively. Interoperability is also addressed in MobiCloud so as to have collaboration between different programs and protocols to make the framework robust and flexible.

2- Dynamic Credential Generation Scheme

Khan *et al.* [5] proposed a light-weight security scheme that dynamically generates security credentials. These credentials can secure mobile user's identity. However, the scheme offloads the work to cloud. The credential sharing process is made among three parties involved in the system. The parties are mobile user, manager and CSP. The credential sharing is made in a secure environment which can avoid Man-in-the-Middle attack.

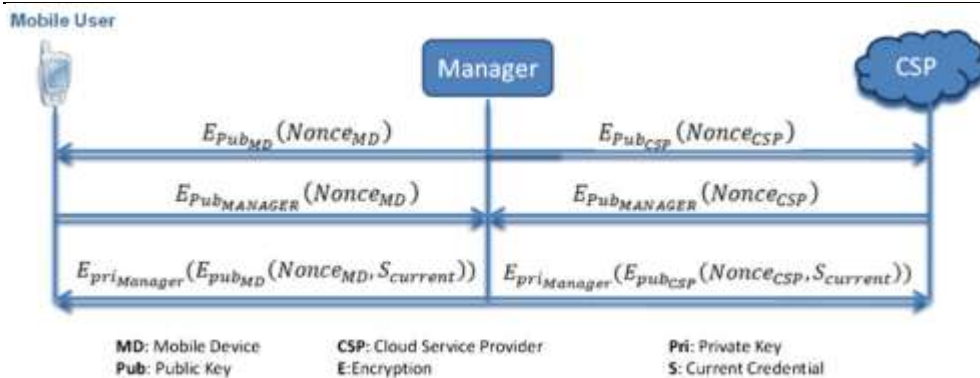


Figure 2 – Dynamic credential sharing [5]

As shown in Figure 2, secure channels communication is fulfilled with respect to the credential sharing mechanism that can withstand potential attacks in mobile cloud computing. The manager involvement in the middle can enhance security in the mobile cloud computing. Here the jobs of mobile users are offloaded to a trusted manager who can take care of operations pertaining to normal data dynamics and also security. The frequent update in the keys makes this solution robust to internal and external threats.

3- ThinkAir Framework

Kosta *et al.* [11] proposed a mobile cloud computing framework which offloads the application functionalities to cloud. It exploits the virtualization concept to leverage Smartphone capabilities. The framework is capable of achieving scalability and security using various mechanisms. The framework assumes that mobile broadband increases from time to time, capabilities of mobile devices increase and sustainability of cloud computing in terms of resource sharing. The design goals of ThinkAir are dynamic adaptation, ease of use, performance improvement, and dynamic scaling.

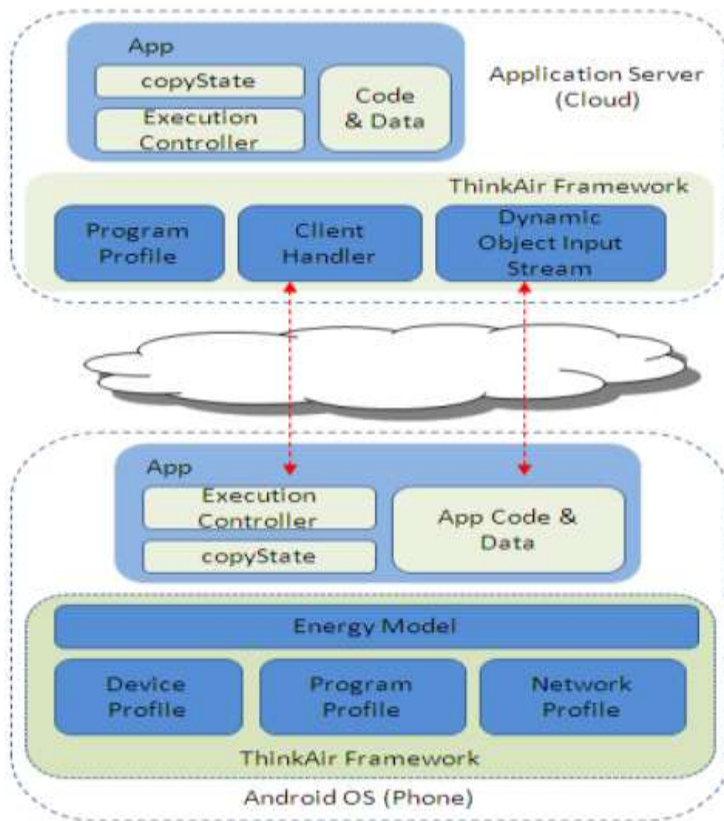


Figure 3 – Architecture of ThinkAir [11]

As seen in Figure 3, the ThinkAir framework has energy model which has provision for device profile, program profile, and network profile. The applications that run in the mobile device can have application code and data, copy state and execution controller. The framework also has client handler, and dynamic object input stream. Secure communications are possible with this framework as it leverages the applications by using security mechanisms supported by Java programming language.



4- Cloud Proxy and Security Level Integration

Ruebsamen and Reich [18] proposed role based access control, five security levels and cloud proxy in order to have secure communication channels between cloud and mobile devices. The five security levels include Level 0 (critical), Level 1 (severe), Level 2 (baseline), Level 3 (Secure), and Level 4 (Highly Secure). Cloud proxy along with these five security levels is employed in order to achieve high level of security. At user level technical and non-technical security is involved. At device level configuration, device properties, and runtime information are involved. At communication channel level access point and encryption are involved. The role based access control can have fine-grained control over the secure access of data in mobile cloud computing. Checking of security level and also access control are combined for robust security mechanism. Two phase evaluation and role based access control besides cloud proxy makes the system to have secure channels between the mobile devices and cloud.



Table 1 the summaries of the strength for each current technique.

N	Author	Technique	Strength
1	Dijiang Huang Xinwen Zhang Myong Kang, Jim Luo	MobiCloud	Provide security isolations to protect mobile users' information. Monitor MANET status for risk assessments, intrusion detection and response. It use Fine-Grained Resource and Security Isolation also Serve as an arbitrator for identity, key, and secure data access policy management.
2	Abdul Nasir Khan Sajjad A. Madani Mazhar Ali	Dynamic Credential Generation Scheme	Proposed scheme reduces the possibility of the Man-in-the-Middle attack due to the involvement of nonce in generating the cloud and mobile secrets. It use the authentication of signature and encrypted with mobile user public key.
3	Sokol Kosta Andrius Aucinas Pan Hui Richard Mortier Xinwen Zhang	ThinkAir Framework	It assume a trustworthy cloud server execution environment (code and state data are not maliciously modification or stolen). Integration lightweight authentication mechanism into the application registration process.
4	Thomas Ruebsamen Christoph Reich	Cloud Proxy and Security Level Integration	It use proxy running in a cloud environment that control the access for mobile device. It use RBAC (role based access control) model has been extend by 5 security levels.



V. CONCLUSIONS AND FUTURE WORK

Mobile devices in the recent past witness dramatic improvements and innovations in terms of features and capabilities. However, they are still having finite resources that cause security issues besides limiting their capabilities. In the wake of cloud computing, the mobile devices can become service nodes that can offload storage and computing to cloud. The whole infrastructure that include mobile networks, collaboration mechanisms and the cloud infrastructure can form mobile cloud. The computing in such environment is known as mobile computing. In this paper we studied the security issues in mobile computing and the possible solutions to overcome the issues. We focused on secure channels transmission in mobile cloud. Two frameworks were discussed in this paper. They are MobiCloud which provides comprehensive security framework for mobile cloud computing and ThinAir which provides an architecture in which mobile devices can offload storage and computing to cloud computing. The paper throws light into various security issues and mechanisms that can be used to overcome the issues. The research on secure channels transmission in mobile cloud computing can be extended further by exploring new framework that can increase robustness and flexibility in secure mobile computing phenomena.



REFERENCES

- [1]. Dijiang Huang. (2010). *MobiCloud: Building Secure Cloud Framework for Mobile Computing And Communication*. IEEE, p1-16.
- [2]. Shih-Hao Hung. (2012). *Executing mobile applications on the cloud: Framework and issues*. Elsevier. 63 (1), p.573–587.
- [3]. Yong Cui · Xiao Ma · Hongyi Wang. (2013). *A Survey of Energy Efficient Wireless Transmission and Modeling in Mobile Cloud Computing*. Department of Computer Science, p.54-76.
- [4]. Yu-Jia Chen. (2011). *A Security Framework of Group Location-Based Mobile Applications in Cloud Computing*. Department of Computer Science (1), p1-16.
- [5]. Abdul Nasir Khan. (2013). *Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing*. J Supercomput, p.793-801.
- [6]. Weiwen Zhang. (2013). *Energy-Optimal Mobile Cloud Computing under Stochastic Wireless Channel*. IEEE, p1-18.
- [7]. Geng Wu. (2011). *M2M: From Mobile to Embedded Internet*. IEEE, p1-18.
- [8]. Hoang T. (2011). *A survey of mobile cloud computing: architecture, applications, and approaches*. Department of Computer Science, p.338-353 .
- [9]. Wenny Rahayu. (2013). *Mobile cloud computing: A survey*. Elsevier. 29 (1), p.84–106.
- [10]. Shih-Hao Hung. (2011). *An Online Migration Environment for Executing Mobile Applications on the Cloud*. Department of Computer Science, p1-23.
- [11]. Sokol Kosta. (2012). *ThinkAir: Dynamic resource allocation and parallel execution in the cloud for mobile code offloading*. IEEE, p.793-801.
- [12]. Abderrahim BOUROUIS1. (2013). *A NEW ARCHITECTURE OF A UBIQUITOUS HEALTH MONITORING SYSTEM:.* Department of Computer Science, p1-10.
- [13]. Carlos Oberdan Rolim. (2010). *A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions*. Department of Computer Science, p1-6.
- [14]. Pragya Gupta. (2012). *Mobile Cloud Computing: The Future of Cloud*. ISSN. 1 (3), p1-9.
- [15]. Peng Zou. (2010). *Phosphor: A Cloud based DRM Scheme with Sim Card*. 12th International Asia-Pacific Web Conference, p.84–106.



- [16]. Piotr K. Tysowski. (2013). *Towards Secure Communication for Highly Scalable Mobile Applications in Cloud Computing Systems*. Department of Computer Science, p1-23.
- [17]. Dejan Kovachev. (2012). *Adaptive Computation Offloading from Mobile Devices into the Cloud*. IEEE, p.499-502.
- [18]. Thomas Ruebsamen. (2012). *Enhancing Mobile Device Security by Security Level Integration in a Cloud Proxy*. Department of Computer Science, p.84–106.
- [19]. Xiaohui Liang. (2011). *An Efficient and Secure User Revocation Scheme in Mobile Social Networks*. IEEE, p1-23.
- [20]. Muhamad Felemban. (2013). *A Distributed Cloud Architecture for Mobile Multimedia Services*. Department of Computer Science, p.54-76.
- [21]. Farshad A. (2007). *Service Clouds: Distributed Infrastructure for Adaptive Communication Services*. IEEE. 4 (2), p.3401 – 3414.
- [22]. Henian Xiaa,. (2012). *Cloud-ECG for real time ECG monitoring and analysis*. Elsevier, p1-18.
- [23]. Ashish Agarwal. (2011). *The Security Risks Associated with Cloud Computing*. ISSN, p.499-502.
- [24]. Issa M. Khalil. (2013). *Security Concerns in Cloud Computing*. Department of Computer Science, p1-23.
- [25]. L A K S H M I S U B RAMANI A N. (2011). *Security as a Service in Cloud for Smartphones*. Department of Computer Science, p1-16.