International Journal of Grid and Distributed Computing
Vol.6, No.6 (2013), pp.37-50
http://dx.doi.org/10.14257/ijgdc.2013.6.6.04

Security Issues and Challenges of Mobile Cloud Computing

Abid Shahzad[1] and Mureed Hussain[2]

Faculty of Computing, Shaheed Zulfikar Ali Bhutto Institute of Science and Technology (SZABIST), H-8/4, Islamabad 44000, Pakistan

a4abishah@gmail.com[1], mhussain@szabist-isb.edu.pk[2]

Abstract

Cloud computing is proving itself an emerging technology in IT world which provides a novel business model for organizations to utilize softwares, applications and hardware resources without any upfront investment. Few years later with the broad development in mobile applications and advancements in cloud computing, a new expansion is being expected in the form of mobile cloud computing (MCC). MCC provides a platform where mobile users make use of cloud services on mobile devices. The use of MCC minimizes the performance, compatibility, and lack of resources issues in mobile computing environment. Despite the astonishing advancement achieved by MCC, the users of MCC are still below expectations because of the associated risks in terms of security and privacy. These risks are playing important role by preventing the organizations to adopt MCC environment. Significant amount of research is in progress in order to reduce the security concerns but still a lot work has to be done to produce a security prone MCC environment. This paper presents a comprehensive literature review of MCC and its security issues and challenges.

Keywords: *Cloud Computing, Mobile Cloud Computing, Security Issues.*

1. Introduction

Cloud computing is an emerging technology which provides IT services and resources to the customers through public network specifically internet. The cloud computing services and infrastructure are mostly owned by a third party called cloud service providers. Cloud computing offers an innovative model for the organizations to use software applications, storage and processing capabilities of cloud without investing on the infrastructure. As compared to existing IT models, the cloud computing offers many advantages like scalability, flexibility, efficiency and non-core activities [1]. Despite these extraordinary benefits of cloud computing, the security is a major concern. According to the International Data Corporation (IDC) survey published in 2009, 74% IT managers and Chief Information Officers (CIOs) thinks that security and privacy issues are the main obstacle preventing organizations to adopt cloud computing services. In the same year a survey conducted by Garter that more than 70% Chief Technology Officers (CTOs) showed their concern about data security and privacy issues in cloud computing [2, 3].

1.1. Cloud Service Delivery Models

The cloud computing model is based on three service delivery models and three cloud deployment models [1, 2, 3, 4, 5].

ISSN: 2005-4262 IJGDC

The three service delivery models are:

Infrastructure as a service (IaaS): In this model the cloud providers offers the cloud services like hardware resources, storage and network infrastructure services. The virtualization is the base of this model.

Platform as a service (PaaS): In this model the cloud service providers provide application development platform for the developers. They also deliver a set of APIs for the developers to develop and launch their own customized applications. They do not need to install development tools on their local devices and machines.

Software as a service (SaaS): This model facilitates the customers to access the applications hosted on the cloud. Instead of installing the applications on their own machines, the users access these applications installed on the cloud using their own browsers. This model can be hosted directly on the cloud or may be PaaS and IaaS.

1.2. Cloud Deployment Models

The cloud has three different deployment models and each model has its own benefits and trade-offs. There is also another model called community model but it is used in rare cases.

Private cloud: This cloud is setup specifically for an organization within its own data center. The organizations manage all the cloud resources which are owned by them. The private cloud offers more security as compared to other two.

Public cloud: This cloud is available to all the external users through internet who can register with cloud and can use cloud resources on a pay-per-use model. This cloud is not secure like private cloud because it is accessible to the internet users.

Hybrid cloud: This is a type of private cloud which uses the resources of one or more public clouds. It is a mix of both private and public cloud.

Rest of this paper is organized as follows: Section II gives an overview of mobile cloud computing and explanation of its architecture. Section III provides the evaluation of existing and proposed frameworks. The issues and challenges of MCC are provided in section IV. Advantages of MCC are presented in section V and some highly rated applications are in section VI. The last section VII concludes with summary.

2. Mobile Cloud Computing

In The mobile cloud computing (MCC) has been inherited from cloud computing soon after the cloud computing era begun around year 2007. MCC incorporates cloud computing properties with the mobile computing environment. Due to its attractive business model and the increased number of mobile phone (smart-phone, tablet pc etc) users in the world, the MCC is proving to be a potential future technology. It has also attracted the attention of many businessmen and entrepreneurs as a prospective and lucrative business opportunity. In [6] MCC has defined as that in MCC all the data, its storage and its processing takes place at the cloud infrastructure instead of mobile device. The mobile cloud applications running on the mobile use the computational power and data storage capabilities of the cloud. Therefore, MCC brings mobile computing services to a wide range of mobile users in addition to the smart phone users.

From mobile user prospective, MCC is an amazing improvement because it diminishes the mobile resources issues like, limited battery power, slow processing power, low internet bandwidth, small storage space and less energy consumption [7]. These mobile limitations always provide barriers for the users to make use of high computation and power consuming applications. However, MCC facilitates low resource mobile devices to use all these applications using mobile cloud resources and services at very low cost. In other words, MCC offers data processing and storage capabilities in the cloud which the mobile user can access using mobile device's web browser. The mobile users do not need high data processing and storage capabilities services on their mobile devices since cloud resources are used for all the data processing and storage. Therefore, the MCC popularity among the mobile users is increasing rapidly and is also highlighted in [7] that ABI research predicts that the number of mobile cloud computing subscribers is expected to grow from 42.8 million (6% of total mobile users) in 2008 to 998 million (19% of total mobile users) in 2014. According to another report of Juniper shared in [8] that the demand of mobile cloud based application is increasing with rapid phase and its market value will raise 88% in the time period of five years from 2009 to 2014.

Despite enormous benefits (like, using cloud servers, network and storages, platforms and softwares services) which MCC offers, the numbers of cloud users are below than expectations. The low number of the cloud users is alarming if we compare it with the advantages which MCC has brought into mobile computing world. The only barrier which prevents the users to adopt mobile cloud computing is the risks in terms of security and privacy of the data and services. Most of the IT executives and managers around the world have security and privacy concerns. A survey conducted by a research firm Portio and published by another research firm Colt points that 68% of chief information officers (CIOs) have serious concerns about the security of cloud computing [9].

2.1. Mobile Cloud Computing (MCC) Architecture

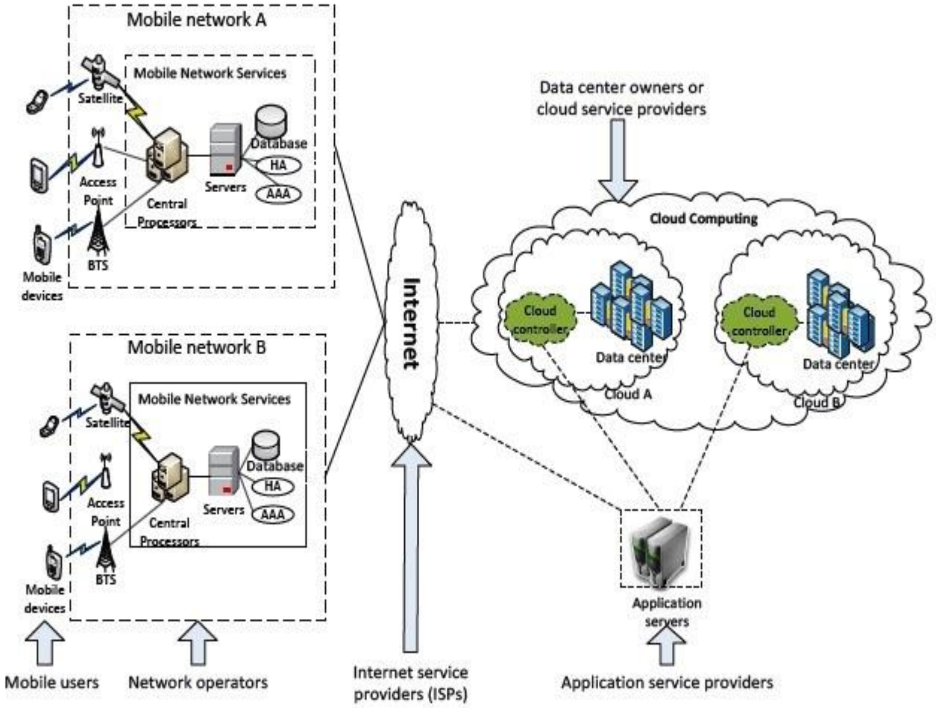

Figure 1. Mobile Cloud Computing Architecture [8]

The architecture presented by [8] is the generic architecture of mobile cloud computing (MCC). The figure shows that there are two different mobile networks A and B. Each mobile network consists of different mobile user devices which are connected to it through wireless access point, BTS or satellite. Different network services like database, Home Agent (HA), Authentication, Authorization and Accounting (AAA) is running on the servers available in the mobile network. The user's request (credentials) is processed by the central processers who are directly connected with the servers. Afterwards, on the basis of HA and the user's information stored in the databases, the mobile network operator provides AAA services to the users. After all this the user's request leaves the mobile network and connects to the cloud (owned by data center owners or cloud server providers) through internet. Once the user enters the cloud, the cloud controller links the user's request with the relevant cloud depending upon the service requested by that user. The user can request different services like virtualization, computing resources, applications, databases and storage services in the cloud.

3. Literature Review

3.1. Evaluation of Existing and Proposed Frameworks of Mobile Cloud Computing

The authors in [4] have provided comprehensive information regarding the cloud security problems. The authors inspected the security problem from cloud architecture point of view, the cloud stakeholders' point of view and at the end from cloud service delivery models point of view. From architecture prospective, the cloud service providers need to provide multi-tenancy and elasticity as both these characteristics play a major role in cloud security.

From stake holder prospective, the security configurations needs to be organized so, each service should be maintained a level and at runtime. From service delivery model prospective, the IaaS, PaaS and SaaS models have security issues. The cloud management security issues and cloud access method security issues are also highlighted.

The authors of [5] have presented an overview of MCC security architecture. Privacy and integrity of the data is important aspect of MCC security. The author categorized the users' in term of security into two categories: mobile network security and cloud security. In first category the security for mobile applications and privacy are explained. The second category is about securing the information on the cloud or simply securing the cloud. In cloud security the authors highlight very important concerns associated with data integrity, authentication and digital rights.

The authors in [2] have provided details about the security issues which cloud service providers are facing when they dig deep for cloud engineering. Therefore, in order to ensure data and application security in cloud environment, the cloud service providers must follow the Manages Service Model (MSP). A detailed survey results which is conducted by International Data Corporation (IDC) highlights that security is the biggest concern of IT executives and other peoples involved in an enterprise's decision to move for cloud services. There are some serious issues and challenges which cloud computing is facing in the domain of cyber security.

The cloud service providers must have to follow the standards like Information Technology Infrastructure Library (ITIL) and Open Virtualization Format (OVF) in order to minimize these security issues and concerns. The paper also covers security management models for the cloud service providers in order to meet security compliance.

The paper [3] presented a detailed analysis of data security and privacy protections issues along with the existing solution to provide protection against these issues. Authors supported their arguments by the surveys from IDCI and Garter. Detailed cloud security architecture has also been explained. The security architecture highlights the infrastructure, platform, software security along with the services related to auditing and compliance.

Cloud computing is facing serious data security and privacy issues which need to be addressed.

In [9] the authors have identified the serious threats and risks related to privacy and security for the mass and corporate users when they will integrate their mobile hand held devices with the cloud infrastructure. The paper points towards the different motivational factors which are forcing mobile cloud operators to move their services and operations to cloud. Some of the key motivational factors are business interest, user demand, preparation of network service provider, QoS and mature technologies. The authors conducted a survey that how wireless mobile devices integrates with the cloud. The people targeted for the survey are mobile device users, cloud developers, IT manager or executives and wireless network administrators. These people are targeted in order to get proper results whether the security and privacy concerns of the users have increased or not if they are planning to move for the cloud.

The results of the survey conducted showed that the privacy of the data is the major concern for the 86% of the normal mobile users and 94% of the IT managers. The paper highlighted the risks in the security architecture when mobile devices will integrate with cloud. It has categorized the architecture into three points where attacks are possible. a) At user device end b) in cloud infrastructure and c) in communication channel.

The author in [10] designed a data service mechanism (SDSM). The SDSM provides best data access control and confidentiality of data stored in the cloud. In SDSM, the data and security management is outsourced to the mobile cloud in a trusted way. The system model is divided into two categories, the network model and the security model.

In network model the data owners, data servers and data sharers are involved. Security model explains that the algorithm used in it ensures that only authorized data sharers can access the data. The proposed SDSM provides benefits like, strong access control, flexibility and low overhead. The algorithm used in model represents in five phases. The first phase contract with setup, data encryption is in second, data sharing in third, access data in fourth and policy updating in fifth phase.

In [11] the authors have explained the security issues related to private data and mobile cloud applications in detail. Keeping the security issues and the existing solution limitations in mind, the authors proposed a mobile computing applications security framework to make sure that the security of the data is achieved when it is transmitted between the components of the same mobile application. The framework also verifies that the integrity of the applications either at the time of installation or updating on the mobile device is intact. The proposed framework best fits in SaaS layer of the cloud service delivery model by providing the security services like confidentiality and integrity using cloud service that provide the same security services.

The authors in [6] have highlighted MCC architecture. After the detailed MCC architecture, the applications of MCC are explained ranging from mobile commerce, mobile learning, mobile health care and mobile gaming.

The existing solutions are also presented in detail. The author also discussed open issues linked with low bandwidth, network access management, quality of service, pricing, and standard interface.

The survey presented in [7] explains MCC very well. The authors explain the existing solution proposed to secure MCC infrastructure and also highlight the uprising issues in MCC. The paper presents MCC architecture along with the overview of the different security services at different layers of the cloud computing delivery service model. At backbone layer, the secure cloud physical services are available. At the infrastructure and supervisor layers, secure cloud process hosting services are available. Secure cloud application services are available at the application, platform and infrastructure layer of the cloud delivery service model. The Paper also describes the criteria before evaluating the existing frameworks for MCC. On the basis of the evaluation criteria a details survey has been produced of existing frameworks. The existing frameworks haven been divided into two frameworks, the application security framework and data security framework.

The authors in [8] have explained the new demands and challenges in mobile cloud computing. They have presented six computing paradigms shift that how computing evolved from internet computing to grid computing and then from grid computing to cloud computing. The MCC model has also been explained in the paper in detail. The novel paradigm shift that mobile cloud computing brought into this world are also highlighted. The paper emphasis on the issues and challenges are given below:

- Performance issues because of intensive applications
- Security and Privacy Issues
- Control Concerns (Because cloud service providers have full control on the platform)
- Bandwidth Costs (High bandwidth is required by the users)
- Reliability Issues

In [12] the paper introduced the concepts of mobile cloud computing, its functionality and different implementable architectures. The authors discussed MCC architecture along with its different services required by the client and servers in the MCC environment from, programming concepts, mobile application framework, specifically mobile data framework and mobile MVC framework is presented in the paper. The architecture for mobile applications in cloud environment has been proposed which explains the services linked with synchronized, push, offline application service, mobile RPC, network, database and inter-app bus needed by the client in MCC.

The authors in [13] introduced a mobile cloud computing architecture and different methods to implement MCC effectively and efficiently. They also investigated the critical issues and challenges persist in the MCC. The authors categorized the MCC solutions into two different categories. The first category in which, a system is constructed which uses the same cloud infrastructure which the users do in order to improve the performance of the mobile devices and a second category in which different applications are developed specifically for mobile devices which employs cloud computing. This second category best fits for the applications like, email or chatting because internet is used as common resource in these devices instead of storage. MCC is facing some potential barriers which are obstacle for shifting from cloud computing to mobile computing which are given below:

- SaaS is the model which is implemented in MCC because of limited storage, less battery, poor display and less computational power of mobile devices.
- There is no proper standard to follow which leads to problems like limited scalability, unreliable availability of service and service provider lock-in.

The authors of [14] have classified two different types of security services a) Critical Security (CS) service and Normal Security (NS) service. The CS service consumes more cloud resources but provides better security and protection. It also produces more reward to the cloud service providers. The authors proposed a Security Service Admission Model

(SSAM) in order to allocate cloud resources properly to the large number of increasing CS and NS service users and also to produce more incomes from these users. The proposed model SSAM is based on Semi-Markov decision process to utilize system resources in efficient way and also to maximize the system rewards for cloud service providers. The SSAM drives the blocking probability of the cloud service and achieve maximum system grow by keeping system expenses and rewards in consideration in the mobile cloud infrastructure.

In [15] a mechanism for improving the security application of cloud computing is proposed. The mechanism is based on dynamic intrusion detection system which dispatches its detectors on the networking system domain through multi layers and multi stages deployment. The mechanism provides wide range of security protection like protection of web sites and pages threats, detection of any intrusion, verification of the database access and security in cloud side, the detection of system side data leakage and some other issues related to processes.

The authors in [16] proposed a new mobile cloud computing framework that gives the functionality of traditional computation services. It is mainly designed to enhance the working of mobile and ad-hoc networks in terms of trust and risk management and routing in secure way.

After the enhancement made by authors in the traditional mobile adhoc network (MANET) model is transformed to a new service oriented model. The newly evolved model treats every mobile node as a service node. The capacity of the service nodes drives the node to offer and use services. The more the capability of the service node, the higher the services it will offer and use. The services have a broad range and they may be storage, sensing or computation services. In order to minimize the concerns enhanced by the mobility, one or more Extended Semi Shadow Images (ESSI) are mirrored on Cloud. The ESSI can be a clone of the device or may be the image of the device which has more resources with improved functionality. In order to provide secure communication the ESSI and mobile node uses Secure Socket Layer (SSL), Internet Protocol Security (IPSec) etc.

4. Issues and Challenges of Mobile Cloud Computing

During the comprehensive literature review of existing and proposed frameworks of MCC explained in previous section, we have been able to synthesize some major issues and challenges of MCC which authors have highlighted. We have categorized these issues and challenges and are presented below.

4.1. Data Security and Privacy Issues

The mobile cloud users have serious concerns about data security in cloud. The data security is the one of the major issue which is main obstacle for the users to move their data to the cloud. Here we have highlighted some common data concerns in the cloud.

1. Data theft risk
2. Privacy of data belongs to customers
3. Violation of privacy rights
4. Loss of physical security
5. Handling of encryption and decryption keys
6. Security and auditing issues of virtual machines

7. Lack of standard to ensure data integrity
8. Services incompatibility because of different vendors involvement

The concerns in cloud computing around data life cycle are also highlighted which needs to be standardized if we want to motivate the users to adopt cloud data services.

1. Generation of Data
2. Transfer of Data
3. Use and Share of Data
4. Storage
5. Archival and Destruction

In addition to the data security threats on cloud side, there are some attacks which are possible at end user mobile device as well.

1. Device Data Theft
2. Virus and Malware Attacks via Wireless Devices
3. Mis-use of Access Rights

From information security point of view in cloud, we have provided some common information security issues of cloud computing like:

1. System Security of Server and Database
2. Networking Security
3. User Authentication
4. Data Protection
5. System and Storage Protection

4.2. Architecture and Cloud Service Delivery Models Issue

Apart from data and information security, the mobile cloud computing have some general issues in terms of their architecture are highlighted below.

1. Computing off-loading
2. Security for Mobile Users/Applications/Data
3. Improvement in Efficiency Rate of Data Access
4. The Context Aware Mobile Cloud Services
5. Migration and Interoperability
6. Service Level Agreement (SLA)
7. Cost and Pricing

The cloud computing service delivery model has its own issues which are highlighted below.

IaaS model security issues:

1. Virtual Machine Security
2. Virtual Machines images repository security
3. Virtual network security

PaaS model security issues:

1. Structured Query Language related
2. Application Programming Interface Security

SaaS model security issues:

1. Data Security Management
2. Web Application Vulnerability and Scanning

4.3. Mobile Cloud Infrastructure Issues

From cloud infrastructure point of view, a variety of attacks are possible on the cloud. Some of these attacks are given below.

1. Attacks on Virtual Machines
2. Vulnerabilities exists at platform level
3. Phishing
4. Authorization and Authentication
5. Attacks from Local Users
6. Hybrid Cloud Security Management Issues

4.4. Mobile Cloud Communication Channel Issues

A lot of improvement needs to be done at the mobile cloud communication channel. The following attacks which exist at communication channel are:

1. Access Control Attacks
2. Data Integrity Attacks
3. Attacks on Authentication
4. Attacks on Availability

In literature review some generic mobile communication side issues have also been pointed out.

1. Low Bandwidth and Latency problems
2. Availability of Desired Services
3. Heterogeneity
4. Limited Resources

5. Advantages of Mobile Cloud Computing

Despite quite a large number of issues and challenges which MCC is facing, there are still many advantages and plus points which MCC provides as compared to traditional IT environment. In this section we highlight some advantages which still make MCC a potential futuristic technology [6].

5.1. Long Battery Output Time

Battery output lifetime has always been a problem in advance mobile device like smart phones, Tablet pc's especially when they execute heavy applications. MCC facilitates the user by executing heavy and time taking applications in the cloud using cloud resources. The execution of applications at cloud end significantly saves the mobile devices battery power.

5.2. Enhanced Processing Power and Data Storage Space

The MCC provides mobile users a platform to store large amount of data on the cloud. The storage space is always a bigger concern for the mobile users which MCC eliminates. The mobile users get storage facility by connecting with cloud through wireless network. The first example of cloud storage services which are provided by Amazon Simple Storage Service (Amazon S3).

5.3. More Data and Application Reliability

Using MCC, the data reliability is increased to a great extent because data is stored and backed up on different servers in the cloud. This advantage of MCC gets rid of the chances of losing data and application on the user's mobile device.

5.4. Scalability

The cloud service providers can expand their cloud services with less effort and modification to infrastructure. They can easily add applications and services without any concern about resource usage.

5.5. Multi-tenancy

Both data center owner or cloud service providers share the same cloud resources to provide different applications and services to the users. The cost is also divided between the two.

5.6. Flexible Integration

In order to handle different user's requests and demands, the cloud service providers can integrate different services through the cloud and internet without much effort.

6. Applications of Mobile Cloud Computing

So far, there are a large number of mobile applications which have taken the advantage of MCC. These applications have made a huge impact on the market and their value has increased a lot. Here are few of them supported by MCC [6].

6.1. Mobile Commerce

MCC made life easy for commerce by providing mobile commerce (m-commerce) using mobile hand held devices. The applications like finance, shopping, ticketing etc are facing some serious challenges because of low bandwidth, complex mobile architecture and serious security risks. However, the MCC provides the solution for these challenges by integrating m-commerce applications into the cloud environment.

6.2. Mobile Learning

The hybrid of electronic learning and mobility gave birth to mobile learning (m-learning). However, issues like high price of mobile devices and bandwidth, low network transmission rate and lack of electronic educational resources are proving to be main obstacle in the way of m-learning. But the cloud provides large storage and high processing capabilities, which introduce the idea of cloud based m-learning and eliminate the barriers of m-learning.

6.3. Mobile Healthcare

The mobile medical applications have so many limitations like, small storage capacity, privacy and security of data etc. However, MCC eliminates the issues of traditional medical applications used for medical treatment. Therefore, the m-healthcare helps the mobile users to access medical resources in efficient way because of the availability of on-demand services on the cloud.

6.4. Mobile Gaming

Mobile gaming (m-gaming) is one the most popular service for the cloud service providers in terms of revenue generation. Usually, all the mobile games require high computing resources like, graphic rendering. However, in the cloud the m-game can off-load game engine which requires graphic rendering to the cloud server. This way, mobile users can only interact with the screen displays on their devices while all other computation is being performed at the cloud servers.

7. Conclusion

Mobile cloud computing (MCC) is an emerging and futuristic technology because of variety of advantages and applications it offers to mobile subscribers. MCC offers data storage and processing capabilities to the resource limited mobile users which makes it very potential technology in near future. In this paper, we have presented a complete understanding of MCC by explaining its architecture, advantages and applications. We have mainly focused on highlighting the issues and challenges of MCC like, data security, infrastructure security and communication channel security. The main idea behind this research is to identify these issues and challenges because they are preventing the mobile users to take on cloud services.

This research is particularly useful for mobile service providers so, that they can improve the security technologies and mechanisms used for cloud security to minimize the user's security concerns. On the basis of the literature review conducted in this paper, we conclude that MCC is regarded to be a potential technology in coming years but currently facing some serious security issues and challenges which limits its adoption among the mobile users.

References

[1] S. O. Kuyoro, F. Ibikunle and O. Awodele, "Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), vol. 3, Issue 5, (**2011**).

[2] K. Popović and Z. Hocenski, "Cloud computing security issues and challenges", MIPRO, 2010 Proceedings of the 33rd International Convention, (**2010**) May 24-28.

[3] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering (ICCSEE), (**2012**) March 23-25.

[4] M. Al Morsy, J. Grundy and I. Müller, "An Analysis of The Cloud Computing Security Problem", In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, (**2010**), November 30.

[5] Soeung-Kon, J. -H. Lee and S. W. Kim, "Mobile Cloud Computing Security Considerations", Journal of Security Engineering, no. 9, (**2012**) April.

[6] H. T. Dinh, C. Lee, D. Niyato and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches", Wireless Communications and Mobile Computing - Wiley, (**2011**) October.

[7] A. N. Khana, M. L. M. Kiaha, S. U. Khanb and S. A. Madanic, "Towards secure mobile cloud computing: A survey", Future Generation Computer Systems, vol. 29, Issue 5, (**2013**) July.

[8] M. R. Prasad, J. Gyani and P. R. K. Murti, "Mobile Cloud Computing: Implications and Challenges", Journal of Information Engineering and Applications, vol. 2, no. 7, (**2012**).

[9] Morshed, M. S. Jahan, M. M. Islam, M. K. Huq, M. S. Hossain and M. A. Basher, "Integration of Wireless Hand-Held Devices with the Cloud Architecture: Security and Privacy Issues", International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), (**2011**) October.

[10] W. Jia, H. Zhu, Z. Cao, L. Wei and X. Lin, "SDSM: A secure data service mechanism in mobile cloud computing", IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), (**2011**) April 10-15.

[11] D. Popa, M. Cremene, M. Borda and K. Boudaoud, "A security framework for mobile cloud applications", 11th Roedunet International Conference (RoEduNet), (**2013**) January 17-19.

[12] S. Singh, R. Bagga, D. Singh and T. Jangwal, "Architecture of Mobile application, Security issues and Services involved in Mobile Cloud Computing Environment", International Journal of Computer and electronics Research, vol. 1, Issue 2, (**2012**) August.

[13] S. S. Qureshi, T. Ahmad, K. Rafique and Shuja-ul-islam, "Mobile cloud computing as future for mobile applications - Implementation methods and challenging issues", IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS), (**2011**) September 15-17.

[14] H. Liang, D. Huang, L. X. Cai, X. Shen and D. Peng, "Resource Allocation for Security Services in Mobile Cloud Computing", IEEE Infocom 2011 Workshop on M2MCN, (**2011**).

[15] C. -L. Tsai, U. -C. Lin, A. Y. Chang and C. -J. Chen, "Information security issue of enterprises adopting the application of cloud computing", Sixth International Conference on Networked Computing and Advanced Information Management (NCM), (**2010**) August 16-18.

[16] D. Huang, X. Zhang, M. Kang and J. Luo, "MobiCloud: Building Secure Cloud Framework for Mobile Computing and Communication", Fifth IEEE International Symposium on Service Oriented System Engineering (SOSE), (**2010**) June 4-5.

Authors

Abid Shahzad

He has done MS-CS from Shaheed Zulfikar Ali Butto Institue of Science and Technology, Pakistan. He has more than 10 years of professional and three years of part time teaching experience. Presently he is working at Askari Bank Limited, Islamabad as Systems Engineer at Data Center. His area of interest includes Networks and Information Security. So, far he has one journal and one conference publication.

Mureed Hussain

He has first graduated B Sc(Hons) in Applied Physics from the university of Sheffield, England. Soon after his first degree, he developed interest for the computer communication technologies. He obtained his M Sc degree in Computer Networks and Distributed Systems from the University of Aix-Marseille-II- Luminy. Later, he obtained his PhD from the University of Paris5-Rene Descartes- in Information Security. Although main research area of Dr. Hussain is Information security, however, with time he has developed interest in sensor networks and light weight security protocols used for low frequency devices. He is an Associate professor at Shaheed Zulfikar Ali Butto Institue of Science and Technology, Islamabad, Pakistan since 2006 and his teaching subjects involve mathematics, computer networks, cyber security and telecommunication systems.