A Review on Security Issues and Challenges of Mobile Cloud Computing and Preventive Measures

Lipika Goel
Assistant Professor,
IMS Engineering College
Ghaziabad

Vivek Jain
Assistant Professor,
IMS Engineering College
Ghaziabad

ABSTRACT
Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements [1]. Mobile Cloud Computing (MCC) is a revolution in the field of mobile world. Mobile cloud computing is the combination of cloud computing and mobile networks to bring benefits for mobile users, network operators, as well as providers of cloud computing. It advantages to mention but a few include scalability, resilience, efficiency, flexibility and many other. Despite the potential gains achieved from the mobile cloud computing, the people are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hamper the growth of cloud. This paper introduces a detailed analysis of the mobile cloud computing security issues and challenges focusing on the computing types and the service delivery types [1].It also presents the various ways of preventing the security issues.

Keywords
Mobile Cloud Computing (MCC), Cloud Computing (CC), Private ,Public, Hybrid Cloud, Saas, Iaas, Paas, Security.

1. INTRODUCTION
Cloud computing is a way to increase the capacity or enhance capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software's as required [1]. It enhances the existing capabilities Information Technology's (IT). In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. Cloud computing provides the next generation of internet based, highly scalable distributed computing systems in which computational resources are offered 'as a service'. The most widely used definition of the cloud computing model is introduced by NIST as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".
Mobile devices (e.g., smart phone and tablet PC) are increasingly becoming an essential part of human life as the most effective and convenient communication tools not bounded by time and place. Mobile users accumulate rich experience of various services from mobile applications (e.g., iPhone, apps and Google apps), which run on the devices and/or on remote servers via wireless networks. The rapid progress of mobile computing (MC) becomes a powerful trend in the development of IT technology as well as commerce and industry fields [2]. However, the mobile devices are facing many challenges in their resources (e.g., battery life, storage, and bandwidth) and communications (e.g., mobility and security). The limited resources significantly impede the improvement of service qualities.

This paper presents a broad survey on Security issues, challenges and their preventive measures of MCC. Section 2 provides a brief overview of MCC including architecture, deployment model, service delivery model and benefits in various applications. Section 3 presents security issues that arise in MCC. Section 4 specifies the preventive measures. Finally, we summarize and conclude the survey in Section 5.

2. MOBILE CLOUD COMPUTING

2.1 Overview
The MCC forum defines MCC as follows: Mobile cloud computing at its simplest refers to an infrastructure where both the data storage and data processing happen outside of the mobile device [2]. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and MC to not just smart phone users but a much broader range of mobile subscribers'. Aepona describes MCC as a new paradigm for mobile applications whereby the data processing and storage are moved from the mobile device to powerful and centralized computing platforms located in clouds. These centralized applications are then accessed over the wireless connection based on a thin native client or web browser on the mobile devices. Alternatively, MCC can be defined as a combination of mobile web and CC [3, 4], which is the most popular tool for mobile users to access applications and services on the Internet. Briefly, MCC provides mobile users with the data processing and storage services in clouds. . Figure 1 shows an overview of the mobile cloud computing architecture.

2.2 Architecture
Mobile cloud computing refers to the usage of cloud computing in combination with mobile devices [5]. It is a combination between mobile network and cloud computing, thereby providing optimal services for mobile users. Cloud computing exists when tasks and data are kept on the internet rather than on individual devices, providing on-demand access. Applications are run on a remote server and then sent to the user. Figure 2 shows working of the mobile cloud computing architecture.

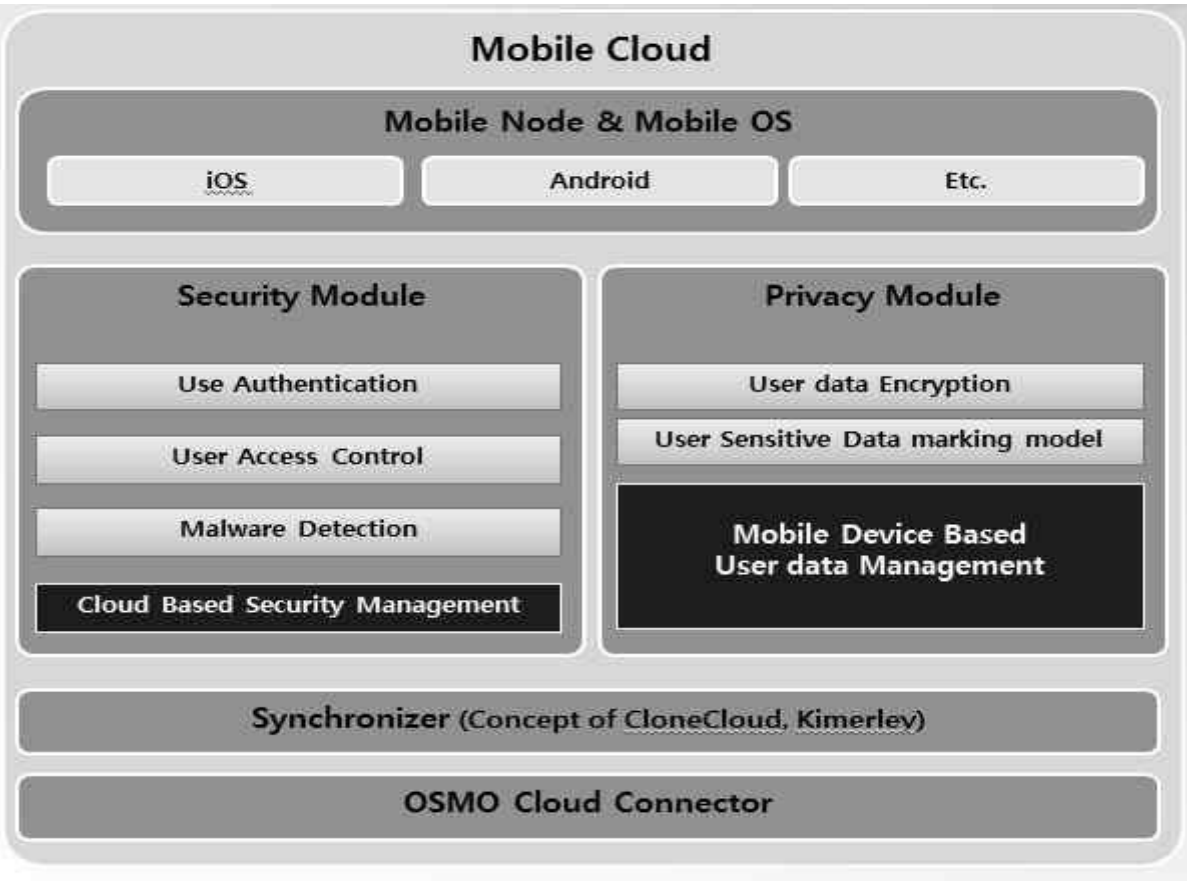

Fig 1: Overview: Mobile Cloud Computing Security Architecture [7]

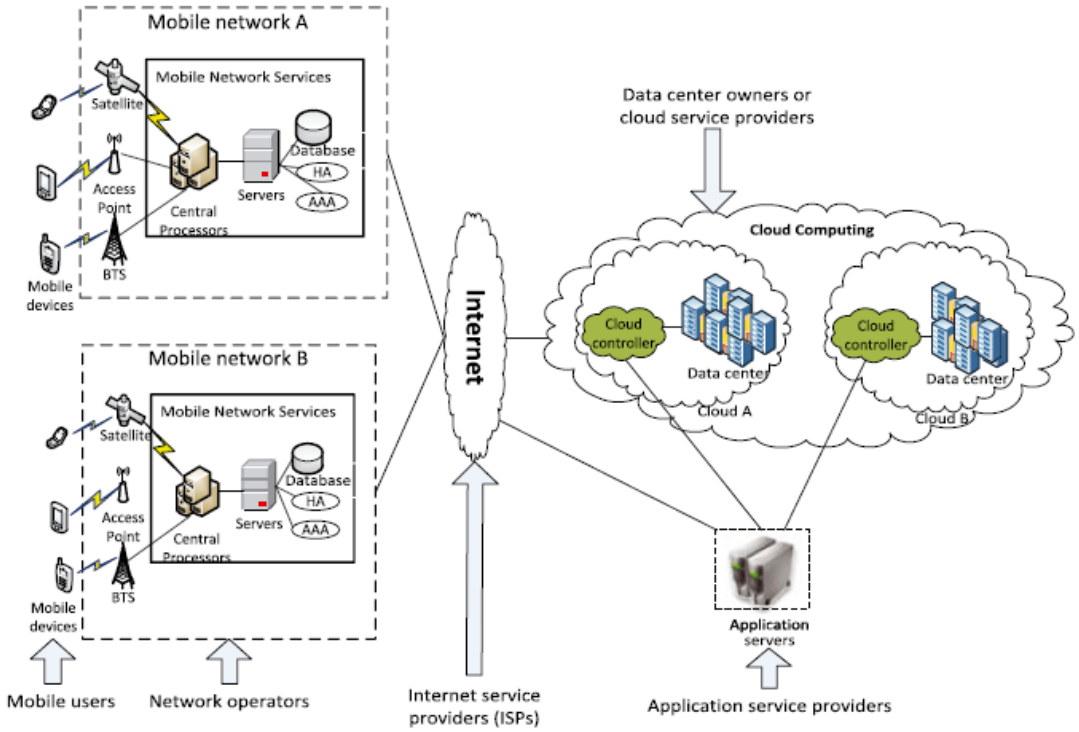

Fig 2: Mobile Cloud Computing Security Architecture [2]

2.3 Mobile Cloud Deployments Models

Networking, platform, storage, and software infrastructure are provided as services in the cloud deployment model that scale up or down depending on the demand [1]. The Cloud Computing model has three main deployment models which are shown in figure 3:

2.3.1 Private cloud

Private cloud is used to define such offerings that mimic cloud computing on private networks. It is set up within an organization's internal enterprise data Centre. The cloud vendor clubbed together scalable resources and virtual applications and made available for cloud users for use as per their requirements. Utilization on the private cloud can be much more secure because of its specified internal exposure. Private cloud has accessed only by the organization and authorized stakeholders.

2.3.2 Public cloud

In public cloud, resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications or web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. It is typically based on a pay-per-use model. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.

2.3.3 Hybrid cloud

Hybrid cloud is a private cloud linked to one or more external cloud services which is managed centrally, provisioned as a single unit, and restricted by a secure network. It provides virtual IT solutions with use of both public and private clouds. Hybrid Cloud provides is more secure that other cloud models and provides secure control of the data and application. It allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems. Hybrid cloud can describe configuration combining a local device, such as a Plug computer with cloud services. It can also describe configurations combining virtual and physical, collocated assets -for example, a mostly virtualized environment that requires physical servers, routers, or other hardware such as a network appliance acting as a firewall or spam filter.

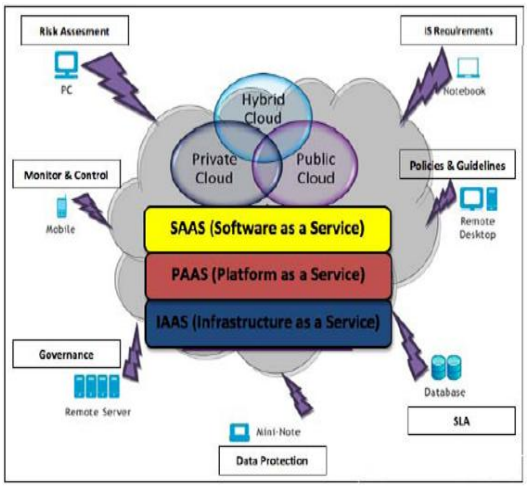

Fig 3: Mobile Cloud deployment model

2.4 Mobile Cloud Computing Service Delivery Models

The three main Mobile Cloud Computing Service Delivery Models are as follows [8] and shown in figure 4:

2.4.1 Software as a service (SaaS)

It is a model of software deployment whereby the provider licenses an application to the customers for use as a service on demand. The End user has the capability to use the provider's applications running on a mobile cloud infrastructure [8]. The applications are accessible from client mobile devices through an interface such as a web browser (e.g., web enabled e-mail). The end users are not responsible to manage or control the underlying mobile cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities. Today SaaS is offered by companies such as Google, Salesforce, Microsoft, Zoho, etc.

2.4.2 Platform as a service (PaaS)

It is the delivery of computing platform and solution stack as a service. The end users has the capability to deploy onto the mobile cloud infrastructure user created or acquired applications which are created using programming languages and tools supported by the provider [8]. The end user does not manage or control the underlying mobile cloud infrastructure including network, servers, operating systems, or storage. PaaS providers offer a predefined combination of OS and application servers, such as WAMP platform [12] (Windows, Apache, MySql and PHP), LAMP platform (Linux, Apache, MySql and PHP), and XAMP(X-cross platform) limited to J2EE, and Ruby etc. Google App Engine, Salesforce.com, etc

2.4.3 Infrastructure as a service (IaaS)

It is the delivery of computer infrastructure i.e. a platform virtualization environment as a service. The end user has the capability of processing, storage, networks, and other fundamental computing resources. The end user can deploy and run different software, which can include operating systems and applications [8]. The user has control over operating systems, storage, deployed applications but they don't manage or control the underlying mobile cloud infrastructure.

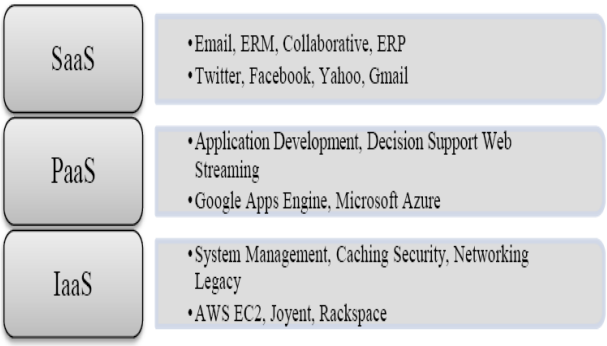

Fig 4: Mobile Cloud Computing Service Delivery Models [4]

2.5 Benefits of Mobile Cloud Computing

Cloud computing is known to be a promising solution for mobile computing due to many reasons (e.g., mobility, communication, and portability). In the following, we describe how the cloud can be used to overcome obstacles in

mobile computing, thereby pointing out advantages of MCC [2].

2.5.1 Improving data storage capacity and processing power

Storage capacity is also a constraint for
mobile devices. MCC is developed to enable mobile users to store/access the large data on the cloud through wireless networks. First example is the Amazon Simple Storage Service (Amazon S3) which supports file storage service. Another example is Image Exchange which utilizes the large storage space in clouds for mobile users. This mobile photo sharing service enables mobile users to upload images to the clouds immediately after capturing. Users may access all images from any devices. With cloud, the users can save considerable amount of energy and storage space on their mobile devices since all images are sent and processed on the clouds. Facebook is the most successful social network application today, and it is also a typical example of using cloud in sharing images.

MCC also helps reducing the running cost for compute-intensive applications that take long time and
large amount of energy when performed on the limited-resource devices. Cloud computing can efficiently support various tasks for data warehousing, managing and synchronizing multiple documents online. For example, clouds can be used for transcoding, playing chess or broadcasting multimedia services to mobile devices. Mobile applications also are not constrained by storage capacity on the devices because their data now is stored on the cloud.

2.5.2 Improving reliability

Storing data or running applications on clouds is an effective way to improve the reliability since the data and application are stored and backed up on a number of computers. This reduces the chance of data and application lost on the mobile devices. In addition, MCC can be designed as a comprehensive data security model for both service providers and users. For example, the cloud can be used to protect copyrighted digital contents (e.g., video, clip, and music) from being abused and unauthorized distribution. Also, the cloud can remotely provide to mobile users with security services such as virus scanning, malicious code detection, and authentication. Also, such cloud-based security services can make efficient use of the collected record from different users to improve the effectiveness of the services.

2.5.3 Dynamic provisioning

Dynamic on-demand provisioning of resources on a fine-grained, self-service basis is a flexible way for service providers and mobile users to run their applications without advanced reservation of resources.

2.5.4 Multi-tenancy

Service providers (e.g., network operator and data center owner) can share the resources and costs to support a variety of applications and large number of users.

2.5.5 Ease of Integration

Multiple services from different service providers can be integrated easily through the cloud and the Internet to meet the users' demands.

3. SECURITY ISSUES OF MOBILE CLOUD COMPUTING

3.1 Major Security Issues

3.1.1 Privacy and Confidentiality

Once the client host data to the cloud there should be some guarantee that access to that data will only be limited to the authorized access. Inappropriate access to customer sensitive data by cloud personnel is another risk that can pose potential threat to cloud data. Assurances should be provided to the clients and proper practices and privacy policies and procedures should be in place to assure the cloud users of the data safety. The cloud seeker should be assured that data hosted on the cloud will be confidential.

3.1.2 Data Integrity

With providing the security of data, cloud service providers should implement mechanisms to ensure data integrity and be able to tell what happened to a certain dataset and at what point. The cloud provider should make the client aware of what particular data is hosted on the cloud, the origin and the integrity mechanisms put in place.

3.1.3 Data Location and Relocation

Mobile Cloud Computing offers a high degree of data mobility. Consumers do not always know the location of their data. However, when an enterprise has some sensitive data that is kept on a storage device in the Cloud, they may want to know the location of it. They may also wish to specify a preferred location (e.g. data to be kept in India). This, then, requires a contractual agreement, between the Cloud provider and the consumer that data should stay in a particular location or reside on a given known server. Also, cloud providers should take responsibility to ensure the security of systems (including data) and provide robust authentication to safeguard customers' information. The movement of data from one location to another location is another issue in mobile cloud computing .Data is initially stored at an appropriate location decide by the Cloud provider. However, it is often moved from one place to another. Cloud providers have contracts with each other and they use each other's' resources.

3.1.4 Data Availability

Customer data is normally stored in chunk on different servers often residing in different locations or in different Clouds. In this case, data availability becomes a major legitimate issue as the availability of uninterruptible and seamless provision becomes relatively difficult.

3.1.5 Portability

All mobile agent runs on a place on the virtual machines called Mobile Agent Place (MAP). Mobile agents carry the application code that move from one MAP to another MAP independent of the CCSP (Cloud Computing Service Provider) there by realizing portability among heterogeneous CCSPs.

3.1.6 Interoperability

Interoperability problem is condensed to the conciliation and association among agents which can be affected using agent interoperability standards.

3.1.7 Mobile network security

Different mobile devices have numbers of security threats such as malicious codes. Some applications to these can cause privacy issues for mobile users .There are two main issues concerning the mobile user security

3.1.8 Mobile Application Security

The easiest ways to check security problems is done by installing and running security software and antivirus on mobile devices. But since mobile devices are having limitation with processing and power, protecting them from these threats could be more difficult compared to regular computers. Several techniques have been introduced for transferring threat detection and security mechanisms to the cloud. Before mobile users could use an application, it should go through some level of threat evaluation. All file activities

that are done on mobile devices will be verified if it is malicious or not. Instead of running antivirus software or threat detection programs locally, mobile devices only performs lightweight activities such as execution traces transmitted to cloud security servers.

3.2 Security Issues in the Service Delivery Model

The security issues in the service delivery model are classified broadly into three sections as follows [5]:

3.2.1 Iaas Issues

3.2.1.1 VM security

Securing the VM operating systems and workloads from common security threats that affect conventional physical servers, such as malware and viruses, using established or cloud-oriented security solutions. Each cloud consumer can use their own security controls depending on their requirement, expected risk level, and their security process.

3.2.1.2 Virtual network security

Sharing of network infrastructure among different tenants within the same server or in the physical networks will increase the probability to exploit vulnerabilities in DNS servers, DHCP, IP protocol vulnerabilities.

3.2.1.3 Securing VM boundaries

VMs have virtual boundaries compared with to physical server ones. VMs that co-exist on the same physical server share the same CPU, Memory, I/O, NIC, and others (i.e. there is no physical isolation among VM resources). Securing the VM boundaries is also an vital responsibility of the cloud provider and it is to be ensured by them.

3.2.1.4 Hypervisor security

A hypervisor is the "virtualizer" that maps from physical resources to virtualized resources and vice versa. Hypervisor is the major controller of any access to the physical server resources by VMs.

3.2.2 PaaS Security Issues

3.2.2.1 SOA related security issues

The PaaS model is based on the Service-oriented Architecture (SOA) model. This leads to inheriting all security issues that exist in the SOA domain such as DOS attacks, Man-in-the-middle attacks, XML-related attacks, Replay attacks, Dictionary attacks, Injection attacks. Mutual authentication, authorization and WS-Security standards are important to secure the cloud provided services.

3.2.2.2 API Security

PaaS may offer APIs that deliver management functions such as business functions, security functions, application management, etc. Such APIs should be provided with security controls and standards implemented.

3.2.3 Saas Security Issues

Enforcing and maintaining security is a responsibility that is shared among the mobile cloud providers and other service providers i.e. software vendors [3]. The security issues discussed in the previous two models also inherits as it is built on top of both of them including data security management i.e. data locality, integrity, segregation, access, confidentiality, backup [8] and network security.

4. PREVENTIVE MEASURES

4.1 Security for mobile applications

Running softwares such as Kaspersky, McAfee, and AVG antivirus programs on mobile devices are the best and simple way to detect security threats on the devices and protect them.

4.2 Refactoring Data

Simply performing the encryption methods does not ensure security in Data Transmission. In case of data transmission , the biggest risk is associated with the encryption technology that is being used. Instead of using encryption and decryption technique data can be broken into small packets and then those packets can be transferred through different paths to the receiver. This practice will reduce the chance of being captured by the unauthorized person. Data is not meaningful unless all the part of the data is received. [4]

4.3 Lockbox Approach

Many storage devices are available these days which has built-in encryption and decryption process, but still security is at risk if the encryption and decryption keys are caught by malicious user. In such a case, a user will be provided a key based on identity management technique corresponding to the COI (community of interest) that he belongs to so that he can have access to the lockbox. To access the data the user needs to acquire the COI key to the lockbox and then he can get appropriate access to the meaningful data. [8]

4.4 Homomorphic encryption technique

Homomorphic encryption techniques are a form of encryption technique which is capable of processing the encrypted data and then bringing back the data into its original form. [9]

4.5 A Hierarchal Proposed System

A hierarchical reputation system [10] has been proposed in the managing trust in a mobile cloud environment.

4.6 Virtualization

Attacks such as denial-of-service can be reduced by Virtualization In virtualization, a single machine is divided into many virtual machines. This technique thus provides better data isolation and safety against denial of service attacks.

4.7 Proxy based architecture [9]

SQL injection attacks are defined as those in which a malicious code is inserted into a standard SQL code. The attackers gain access to a database and are able to access some important and sensitive information. Different techniques like: preventing the usage of dynamically generated SQL in the code, using different filtering techniques to filter the input from the user are used to check the SQL injection attacks. A proxy based architecture to prevent SQL Injection attacks which dynamically detects and extracts users' inputs for suspected SQL control sequences has been proposed in the research paper [9].

4.8 Prevention from XSS Attacks [10]

Dynamic websites get victimized by XSS attacks. It has been observed often that while working on the internet popups open up with the request of being clicked away to view the content contained in them. More often we click on such links and are directed to some other site. Thus the intruding third party gets control over the user's private information or hack their accounts after having known the information available to them. Various techniques for example Content Based Data Leakage Prevention Technology, Web Application Vulnerability Detection Technology has already been proposed to prevent XSS attacks [10].

4.9 Proper SLA

Proper SLAs defining the security requirements such as what level of encryption data should have, when it is sent over the internet and what are the penalties in case the service provider fails to do so.

4.10 Single Sign-On

Single Sign-On In a cloud computing environment, workers log in to multiple applications and services. Because of this reason, it is tedious to implement strong authentication at the user level. To overcome this problem, it is suggested that, to streamline security management and to implement strong authentication within the cloud, organizations should implement Single Sign-On for cloud users. This enables user to access multiple applications and services in the cloud computing environment through a single login, thus enabling strong authentication at the user level.

5. CONCLUSION

Mobile cloud computing is one of the mobile technology trends in the future because it combines the advantages of both MC and CC, thereby providing optimal services for mobile users.

In the field of computing, Mobile Cloud Computing (MCC) has brought a new dimension to Networking Service. The main vision of this service is interconnected "Mobile Cloud" where application providers and enterprises will be able to access valuable network and billing capabilities across multiple networks, making it easy for them to enrich their services whether these applications run on a mobile device, in the web, in a SaaS Cloud, on the desktop or an enterprise server. With this importance, this article has provided an overview of MCC in which its definitions, architecture, and advantages have been presented. This paper have discussed security issues and preventive measures concerning mobile cloud computing. Securing mobile cloud computing user's privacy and integrity of data or applications is one of the key issues most cloud providers are given attention.

6. REFERENCES

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

[2] Hoang T. Dinh, Chonho Lee, Dusit Niyato* and Ping Wang," A survey of mobile cloud computing: architecture, applications, and approaches", Wiley Online Library (wileyonlinelibrary.com), 11 October 2011, DOI: 10.1002/wcm.1203.

[3] White Paper. Mobile Cloud Computing SolutionBrief. AEPONA, 2010.

[4] R. A. Vasudevan, A. Abraham, S.Sanyal, D.P.Agarwal, "Jigsaw-based secure data transfer over computer networks", Int. Conference on Information Technology: Coding and Computing, pp. 2-6, vol.1,April, 2004.

[5] Mohamed Al Morsy, John Grundy and Ingo Müller," An Analysis of The Cloud Computing Security Problem", Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.

[6] Ali Newaz Bahar, Md. Ahsan Habib, Md. Manowarul Islam," SECURITY ARCHITECTURE FOR MOBILE CLOUD COMPUTING", International Journal of Scientific Knowledge, July 2013. Vol. 3, No.3.

[7] Soeung-Kon(Victor) K, Jung-Hoon Lee, Sung Woo Kim," Mobile Cloud Computing Security Considerations", Journal of Security Engineering), Volume(9)Issue(3) :2012.

[8] Seny Kamara, Kristin Lauter, "Cryptographic cloud storage", Lecture Notes in Computer Science, Financial Cryptography and Data Security, pp. 136-149, vol. 60 54, 2010.

[9] A. Liu, Y. Yuan, A Stavrou, "SQLProb: A Proxybased Architecture towards Preventing SQL Injection Attacks", SAC March 8-12, 2009, Honolulu, Hawaii,U.S.A.

[10] D. Gollmann, "Securing Web Applications",Information Security Technical Report, vol. 13, issue. 1, 2008, Elsevier Advanced Technology Publications Oxford, UK.

[11] Mohsin Nazir , Mirza Shuja Rashid , "Security Threats with Associated Mitigation Techniques in Cloud Computing", International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868, Volume 5– No.7,May 2013.

[12] A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT."Platform Computing, pp6, 2010.